NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE COMPONENTS NECESSARY FOR SUCCESSFUL INFORMATION SHARING

by

Jeffrey M. Dulin

March 2009

Thesis Advisor:	Richard Bergin
Second Reader:	Robert Josefek

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2009	Master's Thesis

4. TITLE AND SUBTITLE The Components Necessary for Successful Information Sharing	5. FUNDING NUMBERS
6. AUTHOR(S) Jeffrey M. Dulin	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Charlotte Fire Department 228 East 9th St Charlotte, NC 28202	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	

13. ABSTRACT (maximum 200 words)

The need for information sharing is a growing concern for many agencies in the homeland security field. As communities struggle to prepare for and respond to major incidents, information sharing between agencies is vital. Fusion centers developed around the law enforcement community, which has led to an information-sharing network that is exclusive. Non-law enforcement agencies such as Fire, EMS and Public Health that are charged with preparing for and responding to major incidents need the exchange of information as well. This thesis identifies several components that affect knowledge transfer. The human elements of Relationships, Trust, Megacommunities, Governance, and Leadership form the basis for successful information sharing networks. On this base, the technical components of the information-sharing network such as Standard Operating Procedures, Technology Standards, and Interoperability can be built.

14. SUBJECT TERMS: Fusion Centers, Information Sharing, Governance, Agreements, Relationships, Trust, MOAs, SOGs, SOPs, Technology, Interoperability, Megacommunities, Standards	15. NUMBER OF PAGES 97
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE COMPONENTS NECESSARY FOR SUCCESSFUL INFORMATION SHARING

Jeffrey M. Dulin
Deputy Chief, Charlotte Fire Department
B.A., University of Maryland, 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES (HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2009

Author: Jeffrey M. Dulin

Approved by: Richard Bergin
Thesis Advisor

Robert Josefek
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The need for information sharing is a growing concern for many agencies in the homeland security field. As communities struggle to prepare for and respond to major incidents, information sharing between agencies is vital. Fusion centers developed around the law enforcement community, which has led to an information-sharing network that is exclusive. Non-law enforcement agencies such as Fire, EMS and Public Health that are charged with preparing for and responding to major incidents need the exchange of information as well. This thesis identifies several components that affect knowledge transfer. The human elements of Relationships, Trust, Megacommunities, Governance, and Leadership form the basis for successful information sharing networks. On this base, the technical components of the information-sharing network such as Standard Operating Procedures, Technology Standards, and Interoperability can be built.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The information sharing process between the law enforcement community and the non-law enforcement agencies across the country has not been fulfilling the needs of agencies who, traditionally, have not been involved in the gathering and dissemination of information to support intelligence. The two-way sharing of critical information between these agencies is not occurring on the level that it should be nationwide. The need for a new perspective on how those agencies that are part of the planning, preparation, response to and recovery from a terrorist attack or catastrophic disaster is now. Through an understanding about what is not occurring we can look to create a new vision about what should be happening. We must develop a system that allows information to flow without barriers. This system should enhance information gathering and dissemination both internally and externally.

By conducting research that involved interviews of existing fusion center personnel and a survey of information collectors and consumers, information was gathered that supports the need for a new model. The information that was gathered indicated that there is little cross discipline interaction being conducted in the existing fusion centers. The majority of the information sharing that is taking place is done so on an informal basis through personal acquaintances not established networks. The research indicated that there is a real need to build a system that includes all of the agencies in the information sharing community and is not reliant on human intervention to ensure the information is transferred. Several of those interviewed were of the understanding that there were several barriers to information sharing that were internally generated and not driven by regulations or external requirements. Many of the respondents to the survey addressed concerns that much of the information that is gathered and housed within fusion centers is over classified. This issue creates a barrier that is often used to deny access by non-law enforcement agencies. When questioned, many of the fusion center personnel admitted that very few law enforcement officials

posses any clearances above Law Enforcement Sensitive. In comparison, many fire chiefs, public health directors and other first responder agency administrators' posses equal classifications. The perception of fusion center information sharing as a law enforcement function only is persistent in many of the first responder's opinions. Because of the continued exclusion from being part of the system, many of these non-law enforcement officials surveyed felt that they were not able to perform their duties fully because of the lack of information.

The delineation of authorities at each level of government allows for different views of information gathering and analysis. A national approach to sharing information must be developed and embraced to accomplish this goal. We should look at one system that will incorporate local, state, and national systems into one shared and enhanced system that will be built from the ground up with the goals of all in mind rather than adapting current systems. We need to move beyond the fusion center concept to expand the intelligence community beyond law enforcement and into the areas of fire service, medical community, utilities, and the private sector.

By addressing two major areas of the information sharing community, the human element and the technical challenges, we can build a better system. The human element is comprised of factors that tend to prevent information sharing between people. The lack of trust, relationships, megacommunities, and leadership represent barriers to the development and sustainment of information-sharing systems. These components are necessary to build the base for systems to exist. The administrators and leaders of agencies responsible for collecting and sharing information must buy in to the grander picture of other agencies.

Once good human interaction has been established between agency leaders, there will be a building of trust between them. This philosophy must be pushed down through the organizations to all of those involved in making information sharing occur. The top-down approach to making the system work is vital. The understanding of the Megacommunity theory and the role it plays in building strength through numbers is important. As relationships are built

between agency personnel, the ability to better understand the needs and roles of other agencies will become clearer. To enhance this process, all agencies involved should be part of a governance structure that will guide and approve the processes by which the system will operate. The governance structure has to be made of and include all parties who are expected or need to be involved in any part of the information sharing process. Leadership will be an important aspect that the top-level administrators will have to posses and recognize. Leaders are said to be those people with vision and the courage to reach for their vision. Many times the leadership necessary for an organization to grow or change will come from those closest to the problem. Creative leadership is necessary in the information-sharing network to allow those providing the services the empowerment to provide the organization what it needs to be successful.

The next level of development of the information sharing system has to be built around the technical aspects or components that will allow the information sharing to take place. These may be systems or regulations that grant access, process the information into a useable form or that allow personnel to follow federal guidelines for information handling. The first step is to investigate any standards or laws that apply to information and to list these, and criteria are to follow. This will allow boundaries to be established, which will help identify what can and cannot be accomplished. The next phase of the technical components should be the issue of interoperability and the understanding that all the agencies involved will need to be able to get and share information. Systems that are segregated or protected may need to be evaluated to reveal their true need and what can be adjusted to make them more accessible to others who need and have authority to get the information. The need to build interoperable systems is an important part of the system. The interoperability issue will affect the technology chosen. As the system is built, we must look to the standards of open architecture and Global XML standards so each component of the information-sharing network can be reviewed for pertinent standards and their interdependencies to the entire network.

With technology there will need to be discussions on information assurance and computer security issues. Today we are seeing a new wave of technology that allows for integration of data into a useable format. As we work to become more inclusive in our preparation, prevention, response and recovery from events, we must look at those processes that will allow for better communication systems. The goal of any information system is to get information to those who need the information to enable them to make the most informed decisions possible. Critical information from many sources is imperative when evaluating a decision that affects different agencies. The sharing of information in a real time environment can be accomplished using integrated systems.

The components that have been identified represent a vast majority of the areas needed to build a successful network. It is recognized that there may be others that were not mentioned. There are also many sub-components within each of the mentioned sections that could be explored and expanded upon. To be successful at information sharing, the need exists to recognize that we must look at a wide array of both human and mechanical components. These components all build upon each other and are interdependent to accomplishments of the network. Through evaluation of the components and how successfully we implement each of them, we can determine the likelihood of overall success of the network.

ACKNOWLEDGMENTS

My participation in this program began with the support and sponsorship of the Charlotte Fire Department and the City of Charlotte. I wish to acknowledge my sincere appreciation to Fire Chief Jon Hannan of the Charlotte Fire Department, who has been a mentor and encourager for the last eighteen months. Without his support and understanding, this would not have been possible. I would like to recognize Charlotte City Manager Curt Walton for his support of the Fire Department and its role as the Homeland Security Office for the City of Charlotte. A special “thank you” is extended as well to my fellow deputy chiefs and staff of the Charlotte Fire Department. Without their assumption of my duties throughout my in residence dates, I would not have been able to focus on the work at hand in the program.

The program that has been developed by the CHDS faculty is by far the pinnacle of the academic community. The instructors provided me with a base of knowledge that could not have been explained if tried prior to starting the program. The in-residence sessions were an emersion of topics and issues that exposed me to new ways of thinking of Homeland Security. While in the program, I have gain immense understanding of the political, social, religious and operational aspects of the issue of National Security and Homeland Defense. I want to thank each of the members of the faculty and guest speakers who helped to craft my vision of Homeland Security. This was truly one of the most rewarding experiences of my life and will greatly affect the actions I take in my role as a homeland security professional. I want to personally thank Chris Bellavita and Richard Bergin who were much more than just members of the faculty but were also friends and guides to all of us, which helped to lessen the stress associated with the program.

Over the last 18 months of readings, postings, papers, presentations, in residence sessions in California and a thesis project, I have gained a new set of friends in my fellow students. Without their support and encouragement, I could not have completed the assignments or the thesis. While this program may be ending, the friendship and professional bond with these individuals will continue. I thank you for all that we have experienced together and the strength that we found in teamwork and support for each other. Through the time together, we have made each other stronger and better.

Finally, I would like to say a special thank you to my loving wife Sandy who has been my biggest cheerleader of all. Thanks for the understanding of the long nights at the dinner table until the early hours. The lonely weeks you spent while I was in school in California. I want to thank you for the encouragement and support while working on the assignments and not being able to be with you. Thank you also for being there with me when I thought it was impossible and giving me the strength to finish all the assignments and my thesis. I love you!

I. INTRODUCTION

A. PROBLEM STATEMENT

The information sharing process between the law enforcement community and the non-law enforcement agencies across the country has not been fulfilling the needs of agencies who, traditionally, have not been involved in the gathering and dissemination of information to support intelligence. These agencies can provide new and successful avenues for information gathering. In addition, there is a need to insure that these agencies are part of receiving important information in a timely manner.

Fire service is an example of a non-law enforcement agency that is being excluded from information sharing with other agencies. This includes the two-way sharing of critical information between fire service and law enforcement. Fire service leaders of major metropolitan areas feel there is a lack of involvement of non-law enforcement agencies in the intelligence community as revealed by research for this thesis. This community includes fusion centers, Joint Terrorism Task Forces, and critical infrastructure protection planning. They do not participate in gathering, evaluating, and disseminating information concerning potential terrorism-related intelligence. Fire service agencies need intelligence to properly prepare and respond to threats of terrorism.

One of the major tasks of the fire service is the pre-incident analysis, which takes into account several factors to determine risks and threats. These include the potential situation, available resources, capabilities of personnel, and the coordination of required agencies–all important factors that are part of the pre-incident analysis. Fire service provides much of the incident response capabilities for a weapon of mass destruction-type event, including hazardous materials teams, mass casualty triage, treatment, and structural collapse rescue teams. A terrorist attack may involve a large explosion, the release of chemicals, the destruction of structures, and injury to a large numbers of civilians.

While the fire service is only one of the non-law enforcement agencies that need to be included in information sharing, it is one of the most important because of its role as a first responder. Fire service should have the most up-to-date intelligence on potential threats to properly plan for and prepare the resources needed for potential events.

Understanding that there are several other agencies and disciplines that will also need information to properly prepare for an event, the need exists to evaluate the total picture of who needs what information. In order to make sure that those who have a part in the response–in either the prevention of or the response to an attack–we must look at a new way to assure the dissemination of information.

To accomplish this sharing of information between all agencies that participate in the prevention and response to terrorist attacks, we must develop a system that allows information to flow without barriers. This system should enhance information gathering and dissemination both internally and externally. Information sharing is supposed to take place both within the fusion centers and externally. While this occurs in some centers, between law enforcement agencies at local, state, and federal levels, the inclusion of non-law enforcement agencies is limited or non-existent. The need for integrated and collaborative fusion centers is growing, as many urban areas look to provide timely data\information flow between Joint Terrorism Task Forces (JTTF) and the law enforcement communities. The *National Strategy for Information Sharing,* published by the White House in October 2007, outlined the need to develop an integrated network of information sharing. The *Strategy* recognizes the sovereignty of state and local governments, and thus, the roles and responsibilities are delineated by the understanding that state and major urban area fusion centers are owned and managed by state and local governments. This delineation of the authority of each level of government allows for different views of information gathering and analysis. Furthermore, the incorporation of fusion centers into the intelligence-sharing environment takes into account that these centers support day-to-day

crime-control efforts and other critical public safety activities.[1] Within these fusion centers, there is a need to expand the intelligence community beyond law enforcement and into the areas of fire service, medical community, utilities, and the private sector.

Since fusion centers have mostly been seen as analysis centers, a new approach needs to be investigated that will provide these non-law enforcement agencies with access to the fusion center process. The fusion center process should include linking databases of agencies, providing direct information sharing between agencies, and developing specific intelligence analysis for different disciplines. In some fusion centers, non-law enforcement members could participate at a range of levels. One level is as full members of the JTTF executive committees, where they serve as information nodes for their disciplines. At another level, agencies are contacted about specific issues and provide technical expertise for a subject. A few centers assign members full-time to work side-by-side with non-law enforcement agencies.

Building information systems and fusing them together is one of the major gaps identified by the National Commission on Terrorist Attacks Upon the United States (also known as the 9/11 Commission).[2] A very few fusion centers have full participation from non-law enforcement agencies; most fusion centers include these agencies only as part of a data\information dissemination chain. For the vast majority of fusion centers there is no participation by these non-law enforcement agencies. This creates the need for system that is built on standardization of agencies and disciplines that participate and are included in the information sharing. Some Urban Areas have begun building information centers rather than fusion centers. While fusion centers are designed to receive information and perform analysis on it for linkage and relevance, the information

[1] United States, President George W. Bush, *National Strategy for Information Sharing*, The Whitehouse, October 2007, 10.

[2] Thomas H. Kean and Lee H. Hamilton, *National Commission on Terrorist Attacks upon the United States, Final Report on 9/11 Commission Recommendations* (The 911 Commission Report, Washington, DC, 2004), 401.

centers act as central nodes for activities and vital information flow about incidents. In addition, they may serve as emergency operations centers for small events, which require coordination between all agencies–both law enforcement and non-law enforcement.

The problem with a majority of fusion centers is that they do not include non-law enforcement agencies in the daily operations of information gathering and dissemination. This limits the fusion center's ability to take advantage of the data\information assets to which these agencies may have access. While some centers across the country have some form of non-law enforcement participation, very few actually have full-time staff assigned to them from these non-law enforcement agencies. This lack stems from several reasons that should be examined by each center individually. One reason is that agencies are not being invited to participate due to a lack of available personnel. The lack of technology to support the sharing of information is also a large barrier to current fusion center expansion. Many times this is looked upon as an issue that is beyond the scope of the fusion center's control. In its July 2007 Report for Congress, *Fusion Centers: Issues and Options for Congress*, the Congressional Research Service (CRS) finds that many states lack a state-wide intelligence system with access to databases within their jurisdiction. "Such systems are expensive and potentially problematic in getting all agencies with homeland security-related missions to adopt a particular system." The report cites one of the more advanced fusion centers, which reported having access to only 30 percent of law enforcement data in the state.[3] This report suggests that some fusion centers are not communicating with their own disciplines very well. This is another indicator that there is a fundamental flaw with the basic system. This may be result of a lack of training as well. The Fusion and Law Enforcement Education and Training

[3] Dan Thomas, "Technology Strategy for Second Generation Fusion Centers," *IPublic .org.*, March 28, 2008, http://www.ipublic.org/wiki/index.php/Technology_strategy_for_second_generation_fusion_centers.

(FLEET) Program is designed to help identify training needs with information sharing. This program is sponsored by the Attorney General's Office and provides grants to support this training.[4]

As fusion centers evolve to do more than just the analysis of crime data and leads, a way to receive and disseminate information through new channels will be needed. This will be a difficult task due to a host of issues surrounding privacy of information, clearances of information, and the technology to allow new partners to participate. This may include receiving time-sensitive information, which needs to be distributed immediately rather than analyzed. There will be a need for new technology that will encourage new partners to participate. This new technology may offer a faster, less involved and more cost effective means by which new partners could participate. Some of these new technologies may include secured video teleconferencing, palm devices, and shared portals for information exchange.

As fusion centers gather data and information, there appears to be a lack of involvement by agencies that could provide support to the investigations or analysis. This could be in the form of information from a new, diverse, and previously untapped range of data sets. These could include the following.

- Local law enforcement-related CAD, crime reports, arrests, field interviews, tips and confidential informants
- Local Fire/EMS, DMV, 311, health, transportation, property owners and other operational systems in communities of interest
- Information exchange with other fusion centers, critical infrastructure owners/operators
- Federal information published by DHS, FBI, DOJ, CDC, intelligence community and others via network gateways

[4] Congressional Research Service, *Intelligence and Information-Sharing Elements of S.4 and H.R1*, June 26, 2007, 2.

- Open Source content on Internet web pages, news sites, blogs, RSS feeds, email messages and in office documents (Word, Excel, PowerPoint)
- Commercial sources, such as D&B business data, reverse phone number lookup and others[5]

The data and information sharing (type) governance structures, policies, and procedures of fusion centers will need to be evaluated to determine if they create inherent barriers to data and information sharing. The sharing of information between public and private entities is a new avenue of intelligence that will become even more important in the near future. The private sector can provide access to information that may not be available through public agencies. The use of new technologies may offer new ways to enable fusion centers to better share data and information between agencies that currently do not possess the means. To better facilitate data and information sharing between these agencies, new technologies may need to be designed with specific protocols and systems in mind. To accomplish this, a paradigms shift may need to take place among established fusion center entities. Research on the latest needs of local, state, and federal agencies, will need to be closely directed to ensure support from the established entities.

B. RESEARCH QUESTIONS

- What are the human components necessary for successful data and information sharing between the law enforcement community and non-law enforcement public agencies and private sector partners? How do we structure a system to allow data and information sharing while at the same time providing the necessary critical information protection?
- How can fusion centers leverage technical components such as technology, standard operating procedures, and interoperable systems to enhance data\information sharing? Specifically, how

[5] Dan Thomas, "Technology Strategy for Second Generation Fusion Centers," *IPublic .org.*, March 28, 2008, http://www.ipublic.org/wiki/index.php/Technology_strategy_for_second_generation_fusion_centers.

can various pieces of information, brought together through different technologies, provide interagency and private partners with real time personalized intelligence?

C. ARGUMENT

There is a need to develop uniform methods of data and information sharing that will incorporate non-law enforcement and private sector activities. This information will represent new data sets and intelligence feeds to enhance the current very limited pool of information available to fusion centers. This information could include hazardous materials information, medical transport data, or property inspection data. Fusion centers must incorporate the all-hazards and all-crimes approach in order to exploit the funding and physical assets assigned to them. The missions of fusion centers vary based on the environment in which the center operates; some have adopted an "all-crimes" approach, whereas others have included an "all-hazards" approach.[6] The *Strategy* supports and encourages these approaches, while respecting that a fusion center's mission should be defined by jurisdictional needs. Fusion centers need to evaluate and build successful information sharing systems that address all of the components identified as necessary to achieving their goals. These basic components are the foundation of information sharing. They include governance, standard operating procedures, relationships, and usage, which are required to be successful. The all-hazards/all-crimes approach to information sharing will require the inclusion of multi-disciplinary approaches in the design of any information sharing system whether it is located within a fusion center or outside. The need to utilize technology to communicate with, gather data from, or share information with non-law enforcement agencies has become an issue that must be addressed as fusion centers begin to build their agency base.

The fusion center may also need to shoulder some new responsibilities, such as serving as an information center during events. The center's existing

[6] United States, President George W. Bush, *National Strategy for Information Sharing*, The Whitehouse, October 2007, 15.

information-sharing network could prove to be a valuable tool. Risk assessment tools and site profile programs may be used to identify consequence management models as well. These models could be utilized to help on-scene commands make decisions. There is a need to bring new sources of data and information into the information-sharing system. These new sources can come from those agencies that currently are not participating in information gathering and dissemination.

There needs to be a more proactive approach to engaging more intelligence partners in the information sharing networks of fusion centers across the country. This includes addressing existing barriers such as egos, technology differences, and personnel limitations that prevent centers from including non-law enforcement agencies. The assumptions of many of those surveyed felt that to be effective at interagency sharing of information, requires a physical presence within the fusion center on the part of all agency personnel. However, with the changes in the virtual environment in the last five years, the ability to have presence and access from anywhere has now become a reality. These changes include increased use of mobile and wireless devices to keep personnel constantly abreast of the latest information. In the past, personnel needed to be present in the fusion center to get data and information that now is available almost anywhere. Granted, cyber security is a high priority that has to be addressed; while an important factor in the information sharing system design, security is does not have to be a limiting factor. Information, guidance, and technical support exist to meet security concerns. Attitudes need to change regarding how we gather, share, analyze, and then distribute information once it is used to produce a valuable product

Fusion centers need to change their focus from law enforcement-centric to become more data\information-sharing based. These centers can provide value by evolving into data\information centers as well as fusing information. This would not reduce the analysis of information but rather provide more information flow concerning the analysis. This will accomplish the goal of serving more

customers, such as non-law enforcement and private sector partners, using technology and collaboration processes. By including EMS, fire, public health, and private sector critical infrastructure partners in the data collection and information-sharing matrix, better collaboration can be accomplished. The data presented in this thesis evaluates options for sharing data and information among these new but supportive partners.

D. SIGNIFICANCE OF RESEARCH

The analysis presented in this thesis evaluates the current status of information sharing and provides options for existing and future fusion centers. This thesis examines new ways in sharing data and information between fusion centers and those agencies that are not housed or located within the fusion center. The goal of data and information sharing is to provide those agencies the information that they need to make decisions in a timely manner. To accomplish information sharing in the field of homeland security, a more collaborative information-sharing system will be needed. The goal of the information-sharing system should be to promote information sharing across disciplines in a way that is responsive to the individual needs of agencies and is not limited to personnel having to be located within the fusion center facility.

It is hoped that this thesis will be used to encourage further research into components that are both applicable and practical for implementation. From the data and information gathered in the course of this research, additional recommendations and guidelines can be developed that represent changes in both governance and technology capabilities. As technologies change, the configuration of fusion centers will need to be reevaluated. It is hoped that national baseline capabilities and guidelines will be modified to reflect the information gained through the research presented in this thesis. The linking of local, state, and federal fusion centers in a flexible and secure information-sharing network should be the goal for all local, state, and federal agencies

involved in homeland security. The goal of this thesis is to recommend alternative strategies to national, state, and local homeland security officials to support and embrace the inclusion of new partners into the intelligence community.

II. LITERATURE REVIEW

A review of the available literature reveals a clear consensus that the events of 9/11 demonstrated the need for greater information sharing. There are numerous documents published by established authorities such as federal guidance, congressional testimony (including the 9/11 Commission), literature on smart practices, technical literature, and case studies of existing fusion centers. These materials each address specific areas of need, but fail to provide clear direction on how to accomplish some recommendations. Documents such as the *9/11 Commission Report*, Department of Homeland Security (DHS) / Department of Justice (DOJ) *Fusion Center Guidelines*, the *National Security Strategy of the United States*, the *National Strategy for Homeland Security*, the *Commission on Intelligence Capabilities*, and testimony to Congress from FBI Joint Terrorism Task Forces (JTTF) representatives are among these. The literature can be divided into the following subcategories: work by recognized authorities, congressional reports, national strategy papers, technology reviews, literature on intelligence sharing, and national models of fusion centers.

A. WORK BY RECOGNIZED AUTHORITIES

James Carafano of the Heritage Foundation suggests that state and local representation in the intelligence analysis process is necessary and should be implemented without delay.[7] The National Governors Associations (NGA) Center for Best Practices weighed in on this topic with an issue brief entitled *Establishing State Intelligence Fusion Centers.*[8] Once again, the expansion of fusion center participation beyond law enforcement to include non-traditional intelligence

[7] James J. Carafano, "Terrorist Intelligence Centers Need Reform Now," *The Heritage Foundation*, May 10, 2004, http://www.heritage.org/Research/HomelandDefense/em930.cfm/.

[8] National Governors Association Center for Best Practices, "Establishing State Intelligence Fusion Centers," July 12, 2005, 2, http://www.nga.org/portal/site/nga/menuitem.9123e83a1f6786440ddcbeeb501010a0/?vgnextoid=560a6c6721115010VgnVCM1000001a01010aRCRD&vgnextchannel=4b18f074f0d9ff00VgnVCM1000001a01010aRCRD.

partners such as fire, EMS, public health, utilities, critical infrastructure, and the private sector was deemed critical. The report highlighted Arizona, Maryland, and Georgia as good models of state fusion centers that fully embrace other public safety disciplines.[9] In fact, Maryland's fusion center mission statement includes language specific to the issue: "for the analysis and dissemination of information in statewide support of law enforcement, public health and welfare, public safety and homeland security."[10]

The NGA issue brief made the following recommendation:

> To achieve the cross-functionality necessary for a successful fusion center, states should ensure that the center integrates staff from diverse agencies, including public safety, public health, energy, transportation, technology, the state national guard, etc. Although not all state agencies need to be part of an IFC, the centers should have provision to incorporate, as needed, liaisons from agencies with homeland security interests.[11]

Even today, many state and local agencies feel that information dissemination is a major problem and that further enhancements are needed for the inclusion of non-law enforcement disciplines. Additional work needs to be done in this area to provide adequate guidance for local fusion center personnel to make good decisions. A more defined pattern for establishing the fusion center and its roles and responsibilities is needed.

B. CONGRESSIONAL REPORTS

The 9/11 report was released after evaluation of the actions that led to the events which could have also prevented the attacks. The lack of information sharing was identified as one area that should be strengthened to prevent future attacks. One significant lesson learned from the events of the last seven years is

---

[9] National Governor's Association Center for Best Practices, "Establishing State Intelligence Fusion Centers," July 12, 2005, 2, http://www.nga.org/portal/site/nga/menuitem.9123e83a1f6786440ddcbeeb501010a0/?vgnextoid=560a6c6721115010VgnVCM1000001a01010aRCRD&vgnextchannel=4b18f074f0d9ff00VgnVCM1000001a01010aRCRD, 5.

[10] Ibid., 7.

[11] Ibid., 10.

that state and local agencies are significant partners in homeland security. The war against terrorism has come to include more connectivity between local, state, and federal agencies, combining resources and intelligence for the good of all to provide the level of national and domestic security expected by the people of the United States.[12]

In 2004, the Information Sharing Environment (ISE) was established by the president and the Congress "for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."[13] The ISE supports five communities–intelligence, law enforcement, defense, homeland security, and foreign affairs–by leveraging existing capabilities and aligning policies, standards, and systems to ensure that those responsible for combating terrorism have access to timely and accurate information. Numerous national initiatives have been set forth that provide guidance to the development of the ISE, including the December 2005 *Presidential Memorandum*, which outlines guidelines and requirements to further the development of the ISE. Many of the results of this *Memorandum* were incorporated by the program manager of the Information Sharing Environment into the *Information Sharing Environment Implementation Plan* issued in November 2006.[14]

A report prepared for Congress in 2007 by the Congressional Research Service stated the need to collaborate the information sharing among various disciplines and agencies. This report outlined the value proposition of fusion centers, potential risks fusion centers face, evolution of fusion centers, characteristics of fusion centers, funding issues, federal roles of fusion centers, private sector roles in fusion centers, and the challenges facing fusion centers.

---

[12] National Commission on Terrorist Attacks upon the United States, "Final Report on 9/11 Commission Recommendations," Thomas H. Kean and Lee H. Hamilton, *The 911 Commission Report* (Washington, DC: 2004), 353-356.

[13] United States Congress, Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458-December 17, 2004.

[14] United States Department of Justice, "Baseline Capabilities for State and Major Urban Area Fusion Centers," *Global Justice Information Sharing Initiative*, September 2008, 2.

The value proposition for fusion centers is that by integrating various streams of information and intelligence, including that flowing from the federal government, state, local, and tribal governments, as well as the private sector, a more accurate picture of risks to people, economic infrastructure, and communities can be developed and translated into protective action. The ultimate goal of fusion is to prevent manmade (terrorist) attacks and to respond to natural disasters and manmade threats quickly and efficiently should they occur. As recipients of federal government-provided national intelligence, another goal of fusion centers is to model how events inimical to U.S. interests overseas may be manifested in their communities, and align protective resources accordingly. There are several risks to the fusion center concept–including potential privacy and civil liberties violations, and the possible inability of fusion centers to demonstrate utility in the absence of future terrorist attacks, particularly during periods of relative state fiscal austerity.[15]

C. NATIONAL STRATEGY

In October 2007, the White House released the *National Strategy for Information Sharing: Success, and Challenges in Improving Terrorism-Related Information Sharing*. This strategy provides the executive direction the nation should take in determining the need for complete and coordinated information sharing. The Bush Administration feels that this strategy should set stage for all agencies within the federal government to pursue collaboration with all partners.

> The *Strategy* was developed with the understanding that homeland security information, terrorism information, and law enforcement information related to terrorism can come from multiple sources, all levels of government, as well as from private sector organizations and foreign sources. Federal, State, local, and tribal government organizations use such information for multiple purposes. In addition to traditional law enforcement uses, such information is used to (1) support efforts to prevent terrorist attacks, (2) develop critical infrastructure protection and resilience plans, (3) prioritize

[15] Congressional Research Service, "A Summary of Fusion Centers: Core Issues and Options for Congress," September 19, 2007, 3.

> emergency management, response, and recovery planning activities, (4) devise training and exercise programs, and (5) determine the allocation of funding and other resources for homeland security-related purposes.[16]

The *National Strategy* developed a good baseline for fusion centers to follow in determining the scope of their purpose. From a local perspective the strategy provides little guidance to shape the concept of operations that fusion centers should use to ensure success. The strategy does not provide the direction fusion centers need to become all-encompassing in their information sharing process. The use of technology and its benefits are not an identified part of the strategy.

The *National Infrastructure Protection Plan* (NIPP) was released in 2006 and outlined some of the options to be included in state and local critical infrastructure and key resource (CI/KR) protection plans. These included the following areas of work: (1) ensuring collaboration with other government entities and the private sector using a process based on the partnership model outlined under the NIPP, or an abbreviated form of the model addressing just those sectors that are most relevant to the jurisdiction; and (2) instituting specific information-sharing networks, such as an information-sharing portal, for security partners in the jurisdiction. These types of networks allow owners and operators, and government entities to share best practices, provide a better understanding of sector and cross-sector needs, and inform collective decision-making on how best to utilize resources.[17]

D. TECHNOLOGY REVIEW

Not enough research has been done within the fusion center community to improve the technology for information dissemination in a secured fashion. This secured means of data sharing is necessary to support the transmission of

[16] United States, President George W. Bush, *National Strategy for Information Sharing* (The Whitehouse, October 2007), 10.

[17] Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Government Printing Office, 2006), 168.

information within a fusion center environment. There is general agreement among non-law enforcement agencies that further enhancements are necessary to provide access. Jim McKay, of *Government Technology* magazine, made the following observation:

> Changes (in information dissemination) include improving the way information is shared with state and local officials–which has improved somewhat since 9/11, with the advent of the Homeland Security Information Network (HSIN) and as a result of Joint Terrorism Task Forces. Virtual fusion centers will require greater security; however, the successful use of technology to operate EOCs has paved the way for the use of more advanced and secure technology systems.[18]

The current available literature on the technology being used in fusion centers is very limited. Many fusion centers are using some form of technology to share information within the fusion center or to notify members of fusion centers that they have new information. There are very few who have expanded beyond these applications to build networks outside of the traditional law-enforcement system. Most of the literature on the use of technology is focused on emergency operations centers, which share some characteristics with fusion centers. The National Institute of Standards and Technology produced a bulletin that provides guidance and is helpful in determining levels and types of security. Information technology security product categories are covered in this document, with a discussion of the types of products, product characteristics, and environment considerations for each category.[19] The building of an information or fusion center is a small part of information gathering and dissemination. There exists the need for a system to gather and distribute information in a timely manner, which meets all safeguards and security issues.

---

[18] Jim McKay, "The Security Shuffle," *Government Technology* (November 4, 2005). http://www.govtech.net/magazine/channel_story.php/97157.

[19] Timothy Grance, Marc Stevens, and Marissa Myers, *Guide to Selecting Information Technology Security Products: Recommendation of National Institute of Standards and Technology*, Special Publication 800-36 (Maryland, National Institute of Standards and Technology, October 2003), http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf.

The lack of interoperability of systems in use today in different fusion centers is an issue that has yet to be addressed**.** There are areas of concern relating to these information management systems. Specifically, there is a lack of coordination regarding the adoption of such systems nationally. In many cases, statewide intelligence systems cannot work in conjunction with other systems within the state or regionally. Despite federal efforts to promote the use of Extensible Markup Language (XML) as the standard format across levels of government for justice and public safety information management systems,[79] fusion centers and states continue to purchase systems that operate using proprietary language and that cannot "speak" to other systems without additional equipment and costs. This may be due to the lack of mandatory guidance on this issue and other technology-related concerns. Currently, all guidance on this is voluntary.[20]

Another issue within the technology realm is the multiple sites and systems that local fusion centers must log into or maintain to receive information. This is a major barrier to information sharing and appears in some instances to create silos of information that are not shared across disciplines or sectors. In addition to funding concerns, the most consistent and constant issue raised by fusion center officials relates to the plethora of competing federal information sharing systems. Fusion centers report numerous sites that federal agencies use that need to be check in order to receive information from the federal law enforcement and other intelligence communities. The Homeland Security Information Network (HSIN) and its sister systems HSIN-Secret and Homeland Security Data Network (HSDN) have been the focus of much controversy in recent years. The lack of consolidation of information on these systems as well as the lack of use were a focus of a report to Congress.[21] Law Enforcement

[20] Congressional Research Service, "A Summary of Fusion Centers: Core Issues and Options for Congress," September 19, 2007, 8.

[21] "The Homeland Security Information Network: An Update on DHS Information Sharing Efforts," Statement for the Record before the House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, September 13, 2006, 2.

Online (LEO), a Federal Bureau of Investigations (FBI)-sponsored website, is an attempt to include FBI in state and local information sharing systems. The Federal Protective Service (FPS) portal and Regional Information Sharing Systems (RISS)–among others–are systems that are segregated in providing information.[22]

E. INTELLIGENCE-SHARING / FUSION CENTERS

Jim McKee wrote that "many officials charged with protecting local communities continue to express frustration that intelligence is too often tardy and lacking detail by the time it reaches states."[23] Representative Jane Harmon, 36th District of California, wrote in a statement to the House Sub-Committee on Intelligence, Information Sharing and Risk Assessment that "These centers–staffed by police and sheriffs' officers, public health authorities, private sector representatives, and others–are an effective 'ground up' response to the need for more and better information about terrorist threats so communities can prepare and prevent."[24]

The lack of participation experienced by many state and local officials has created the push in many of the Urban Area Security Initiative (UASI) cities to spend large amounts of funding to create their own information and fusion centers. At the UASI Conference held in Charlotte, N.C. in April 2008, many of the comments during the Fusion Center/Information Sharing Sessions were centered on the lack of participation by non-law enforcement agencies. This feeling of non involvement of these agencies has many federal officials, believing this has created discord between federal agencies and those local law enforcement agencies who are managing these centers. The lack of national

[22] Congressional Research Service, "A Summary of Fusion Centers: Core Issues and Options for Congress," September 19, 2007, 10.

[23] Jim McKay, The Security Shuffle," *Government Technology* (November 4, 2005), http://www.govtech.net/magazine/channel_story.php/97157.

[24] Jane Harman, Chairman of the House, *The Way Forward on Fusion Centers: Challenges and Strategies for Change*, Committee on Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, Thursday, September 27, 2007, 1.

standards for the design and operation of fusion and information centers has led to these centers being based on local or state decisions rather than on a national design.

Col. Mike McDaniel reviewed the Michigan Intelligence Fusion Center as one potential fusion center design.[25] The Michigan Intelligence Fusion Center has developed the most advanced use of virtual technology for fusion centers.[26] Their approach is to incorporate the Michigan Criminal Justice Information Network (MiCJIN) into the fusion center while using emergency management software to assign critical tasks.[27] In his review, many technology uses are discussed that link information systems for a single point of sharing. This concept is one that needs to be reviewed more to determine other aspects for dissemination of the information generated. In the MiCJIN, the focus is on desk assignments to a diverse group of disciplines. This is probably the biggest leap in fusion center progress because it addresses the need to identify all disciplines and assign roles and responsibilities.

Several articles and guides are available that identify technologies that offer promising solutions to gathering and sharing information and linking databases. There needs to be more literature on the success stories and the suggestions for future fusion center development. More research on centers that are operational and have had success is needed to provide a basis for operational acceptance. Because each jurisdiction is different, there needs to be more of a range of proven models that developing centers can review and select from.

The U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative's (Global) *Fusion Center Guidelines,* provides guidance to

---

[25] Michael C. McDaniel, Emad (Al) Shenouda, and M. John Bustria, "The Functional Desks as Collaborative Mechanisms in the Michigan Intelligence Operations Center," *Homeland Security Affairs*, Supplement no. 2 (2008), http://www.hsaj.org/?article=supplement.2.4.

[26] Ibid.

[27] Ibid.

ensure that fusion centers are established and operated consistently across the country as they relate to handling of information. Using the *Fusion Center Guidelines,* as well as identified best practices, federal, state, and local officials identified the capabilities and standards necessary for a fusion center to be considered capable of performing basic functions. These guidelines should be used to ensure that fusion centers are established and operated consistently, resulting in enhanced coordination efforts, strengthened partnerships, and improved crime-fighting and antiterrorism capabilities. The guidelines and related materials will provide assistance to centers as they prioritize and address threats posed in their specific jurisdictions for all crime types, including terrorism. In addition, the guidelines will help administrators develop policies, manage resources, and evaluate services associated with the jurisdiction's fusion center.[28]

The U.S. Department of Justice's Global Justice Information Sharing Initiative later produced a report on the baseline capabilities for fusion centers. This document identifies the baseline capabilities for fusion centers and the operational standards necessary to achieve each of the capabilities.[29] This document is a huge step forward in setting national standards for the building of fusion centers. By establishing baseline capabilities, those centers have objective based goals that can be measured. While this document along with its predecessor were leaps forward, there still exists the need to establish national requirements for participation in fusion centers.

F. NATIONAL MODELS OF FUSION CENTERS

The only national model to date is the Terrorism Early Warning Group TEWG. This was a program started in Los Angeles in 1996 to fill a gap in

[28] United States Department of Justice, "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," Global Justice Information Sharing Initiative, April 2006, 3.

[29] United States Department of Justice, "Baseline Capabilities for State and Major Urban Area Fusion Centers," Global Justice Information Sharing Initiative, September 2008, 2.

information about terrorists and terrorist activities. The goal of the TEWG was to create a common operating picture for a national network of sharing terrorist threat- and incident-related information and intelligence.[30]

The TEW concept involves the establishment of regional, multi-agency, multidisciplinary mechanisms for sharing, fusing, and assessing information and intelligence. Each individual TEW is an organization based upon collaboration among state, regional, and local law enforcement, fire service, health, and emergency management agencies and organizations. TEW groups build on the core competencies and missions of participating agencies. They bring together the players responsible for addressing terrorist threats and concerns in their areas of operation and to subsequently develop, process, and share the information needed for all phases of counterterrorist operations and with all relevant federal, state, regional, and local entities.[31] This is a model that most fusion centers might look at to develop. The fusion center can take the collaboration of the TEW and expand upon it through greater analysis capabilities. Fusion centers typically house one or more analyst who can compare and contrast information sets as well as determine relevance to information.

Besides the TEWG, no other national models are available. One of the problems with this lack of options is that a fully developed TEWG program is not feasible for many jurisdictions because of financial constraints. While there are a few models such as Los Angeles, Arizona, Maryland and Georgia that offer proven alternative solutions for fusion center inclusion of non-law enforcement agencies, these are exceptions to the standard state fusion center concept that currently is being used. When building a fusion center program, most executives want to base their decisions on the success of other centers before committing the resources and funding.

---

[30] National TEW Resource Center, *Resource Guide: Book One*: *TEW Concept and Overview* (Los Angeles, CA: National TEW Resource Center, January 2005), http://www.ojp.usdoj.gov/odp/docs/Resourcebook1_TEW.pdf.

[31] Ibid.

G. CONCLUSION

The need to provide new and better ways to share information has been addressed as a high priority by all levels of government, recognized authorities, and reviews of past failures. The lack of adequate literature on successful means to accomplish this means many developing fusion centers are struggling to create their identities. This will continue to be a problem until more centers are up and running and are able to report on their successes and failures. One avenue to facilitate open discussion of the issue may lie in informal networks that are developed by operational personnel. The hope is that platforms such as the National Fusion Center Conference and the Urban Area Security Initiative Conference will foster discussions that will foster this exchange of knowledge. These platforms offer opportunities for law enforcement and non-law enforcement agencies to exchange ideas, solutions, and experiences that can lead to changes in designs. The goal is to allow non-law enforcement agencies the opportunity to become part of the information sharing system by showing the relevance they bring to the total intelligence community. Through demonstration and examples of successful programs, the intelligence community can stretch the current boundaries that seem to be limited to the law enforcement community.

III. METHODOLOGY

A. POLICY ANALYSIS

This thesis uses a policy analysis to research the applications of information sharing. The need to understand the methods of sharing information as well as the need to share information is analyzed to gain understanding of the current status of fusion center operations. Currently there are no standards for how fusion and information centers should design their information-sharing systems. While there are standards that outline the gathering, processing, and storage of intelligence information, there is no blueprint from the Department of Homeland Security or any other agency as to how fusion centers should be built to operate most effectively. A document published in September 2008 by Global, entitled *Baseline Capabilities for States and Major Urban Area Fusion Centers,* relates to the functions of fusion centers more than who should be participating in information sharing.

B. DATA COLLECTION

The policy analysis for understanding the need for changes in the information-sharing systems between agencies and fusion centers focuses on current capabilities. Many of the components to successfully collect and share information are not being employed fully based on the data collected in the research for this thesis. To accomplish the analysis, the thesis uses several processes of research to identify what components must be understood by all stakeholders of the information-sharing system. Using different research tools, information was gathered on the current state of information sharing and then translated it to the next tier of qualitative analysis. This process utilized a two-part approach to research the status of information sharing. The first entailed interviews of existing fusion centers managers and information technology

personnel. The second was a blind survey of information users on what information they are currently receiving and how they interrupt the quality of that information.

The population accessed for this research was individuals who have roles of administration or use of the information-sharing networks. This population includes fusion center managers, intelligence analysts, agency heads, emergency management directors, and prevention and response officials. This cross section of information producers and consumers represents the full range of the fusion center and response personnel. Ten currently operating fusion centers were selected and phone interviews were conducted with the fusion center manager and the person responsible for information technology.

The fusion centers are members of the Southern Shield Fusion Center Group. This group represents the southeast States that are working together to build and share information through their fusion centers. The Southern Shield consortium has both small and large population states as members and so replicates a cross-section of fusion centers across the country.

The respondents were sent a list of questions along with the scope of the thesis for all survey participants to review and prepare for the interview. The questions explored the operations of the fusion center and the involvement of agencies that do not have a physical presence in the building. The questions focused on exploring what technologies these fusion centers are using to incorporate these agencies. The participants were also queried (at a later point) as a review panel on the findings and recommendations. A representative from DHS Information and Analysis was interviewed to gain a federal perspective. While this information is of a classified and sensitive nature and was not included in the thesis, the insight gained led to further research in other areas. This research led to specific questions for identified participants about particular instances and cases that supported the research. The information that would be gathered would provide supporting evidence on how well information sharing is taking place.

The findings of the interviews were analyzed by comparing the responses using several criteria: size of the fusion center staff, number of agencies involved, and current level of technology used to share information outside of the fusion center, and who they are currently not able to share information with because of the lack of technology. The make up of each fusion center has a direct impact on the center's priorities. The demographics of each fusion center were compared to the responses by each fusion center to evaluate any relationships that exist. The research should show where there are similar participation and oversight between fusion centers. Through analysis, common issues between all of the respondents were also identified.

The survey respondents came from sending the survey to two different groups. The first is the chief executives of agencies, representing different disciplines from across the country in order to get a cross-section of results. These chief executives were drawn from the Urban Area Security (UASI) and State Administrative Agency (SAA) point-of-contact list provided by the Department of Homeland Security. The chief executives were instructed to have someone within their agency to complete the survey. The names and positions of the respondents was to be withheld from the research to ensure anonymity. The second group receiving the survey link was members of the UASI discussion list which includes over 1,500 members. Using this list, allowed for anonymity of the respondents because there identities would be hidden from the research. The information gained from these interviews and surveys identified trends across different fusion centers and disciplines. The interview questions allowed the respondent to elaborate on their specific operations and policies while addressing the question. In addition, the interviewees had the opportunity to add pertinent points that were not brought out from the questions. This allowed the conversations to be directed around specifics of each center. The survey was conducted by a response submission by the respondent to a survey tool. The results were collected by using a survey tool online. The potential survey respondents came from a large base of multi-agency and multi-discipline

personnel. Using the two different tools of interviews and surveys, allowed for the different questions to be applied in various forms. The interviews questions were asked if a way that did not appear to be questioning the respondents policies or their decisions to conduct their operations in a certain way. This was important to ensure that the respondents openly answered the questions and provided the needed information. The survey questions were arranged in a manner that had the respondent selecting from predefined answers. Because the survey is blind, respondents were able to answer questions that might be seen as harsher. This allowed the survey analysis to identify controversial issues in the information sharing community.

The data collected through the interviews and surveys provided a picture of the current capabilities of the partners of these fusion centers from the interviewee's perspective. Analysis of the data made it possible to derive a course of research to investigate possible solutions. The policy analysis made it possible to design the questions to better fit the respondent's agency. Understanding that the desired responses may not be able to be obtained from the first attempts at interviews, the interviews were conducted in three phases. After the first phase, the findings and data were analyzed to determine the value of the content. From this, the design of the questions was adjusted where needed as was the way in which they are presented. After this adjustment, the second phase of interviews was conducted with a new set of interviewees. Again, the results were analyzed and changes were made as necessary to accomplish better results before the third set of interviewees were interviewed. This modification allowed the author to refine the focus of the interviews and achieve the data needed for the research.

C. DATA ANALYSIS

The information from the interviews was used to identify patterns in the operations and policies of fusion centers. This portion of the research was an attempt to capture those components of fusion centers that are being done the

same way across centers around the country. A compare and contrast analysis identified the processes that are being used consistently across the different centers interviewed. Another aspect of the interview analysis was extracting the specific differences between the centers that the respondents felt made their center better in its function. By allowing the respondents the freedom to discuss specific aspects of their centers operations or policies, better data was captured from their perspective. This allowed for interpretation of results from the centers that may not be obtainable by other means.

The survey analysis drew from a large group to establish a broader perspective. A trend analysis from the data can be identified for mapping across the different types of centers. Survey results were reviewed to identify any abnormalities that could flaw the results of the data. Careful evaluation of the questions and the resulting responses were compared to ensure that the questions, gave the desired response. Both the interview and the survey were used to evaluate the current operations of both the fusion centers and those constituents that rely on the fusion center for information. This two-prong approach gave the research project a view of each side of the information sharing community. The interviews represent the producers of information and the analysis of how it is to be used. The survey represents the consumers of information and how much and of what quality the products produced have. This methodology allowed the research to identify additional characteristics of information sharing and the systems that are currently being used.

While there was a certain group identified for the interview process, some centers did not respond to the request to participate. One center contacted did not feel that this was an appropriate research project and refused to participate. While this is understandable, it did call to question what that center might have contributed to support the thesis. The survey tool response was as expected with a 10 percent response from the base of potential respondents. The response to

the survey was heavy in the emergency management area, which could have been a product of those individuals who are more engaged in the homeland security activities in most communities.

IV. ANALYSIS

A. ANALYSIS PROCESS

The process by which information is disseminated is an important part of the information sharing system. The Global report identified two requirements that should be part of the information dissemination plan.

- The plan should be consistent with the intrastate coordination plan.
- The plan should consider a variety of methods to distribute information, including a website; e-mail; secure portal; regional and national information sharing systems such as Regional Information Sharing Systems (RISS), Homeland Security Information Network (HSIN), Law Enforcement Online (LEO), and HS SLIC; pager; fax; telephone; video teleconferencing system; and personal contact.[32]

B. INTERVIEW ANALYSIS

The results of the interviews conducted with the fusion center directors showed a pattern of how most fusion centers currently operate under a law enforcement-centric organization. The majority of interviewees expressed concerns about the ability to sustain the current capacity without involving new agencies. The need to expand the involvement is looked at as a possible avenue that may provide new funding streams by involving new agencies that may possess other funding options.

One fusion center director had a very unique perspective of the value of including non-law enforcement agencies in the collection of data.

> We do not know what we are missing until it has happened. Fusion centers need to get all of the information and then decide what is valuable at that time and what may be used later. The ability to go ask for information is very difficult when there is not a system and relationship in place that has already built the path.

This comment demonstrates that information sharing is more about the ability to get information when it is needed than the actual information received.

[32] United States Department of Justice, "Baseline Capabilities for State and Major Urban Area Fusion Centers," *Global Justice Information Sharing Initiative*, September 2008, 20.

Several of the interviewees' centers did not have active participation from any non-law enforcement agencies, but did have contact information for those agencies. When asked, "who the fusion center would contact in those agencies not present to get information," they did not have a specific name–merely a phone number of an office. This shows the need for a more formal and established system to ensure the appropriate person is identified for obtaining specific information.

One of the persons interviewed felt that the inclusion of non-law enforcement agencies should be required in fusion centers with the caveat that those agencies be trained in intelligence analysis. This brings up an important point that was discussed with several of the interviewees: "What sort of training and qualifications should all personnel within a fusion center should have?" Several interviewees pointed out that there are standards in place for handling sensitive information and records. It was felt that all personnel should have Protected Critical Infrastructure Information, PCII training to ensure sensitivity of private sector information. In addition, the collection, storage, and retention of all materials within the fusion center must follow the requirements of 28 CFR Part 23.[33] This regulation prescribes what can and cannot be collected and how to protect that information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disasters.

During the interviews, several consistent factors were identified among the agencies involved in the interviews. These factors appear to drive the direction of the centers and the amount of involvement by other agencies outside of the law enforcement community. The directors interviewed represented law enforcement-centric as well as all hazards-approach centers. Five distinct patterns emerged from these interviews.

[33] William J. Clinton, President of the United States, "Criminal Intelligence Systems Operating Policies," *Executive Order 12291*, 1998 Policy Clarification, 1993 Revision and Commentary.

1. The Fusion Center's Location Influences its Major Focus

The majority of centers located within state law enforcement agencies had well-established connections and information sharing systems with the federal-level agencies, but had moderate or low connectivity with local law enforcement agencies. The use of emailed bulletins was the leading and most extensive approach to information sharing that was identified among the state fusion centers. Some of the centers did include non-law enforcement agencies on their email distribution list but did not have direct contacts to these agencies. These ranged from a desk number to call or a generic email address. This lack of specificity leads the researcher to question the effectiveness of this arrangement. Because of the law enforcement orientation of the center, many interviewees expressed a reluctance to send material to non-law enforcement agencies. One aspect of the fusion center's location was the reluctance to use the center as a nucleus to bring outside agencies in for meetings or briefings. The location of the center within the building of a law enforcement agency may be inviting to law enforcement agencies, but it appears to be intimidating to other agencies. Access to the center is complicated when agency personnel must sign in and be escorted through the building to reach meeting rooms or the center itself. While security within a police or sheriff's office is required, the location of the fusion center within this secured building creates additional obstacles to information sharing practices.

2. A Fusion Center's Leadership Guides the Focus of Involving Agencies

The leadership of all the centers interviewed is law enforcement-based. This is representative of the basic conception for current fusion centers since the fusion center concept was born from the law enforcement community. Only a few of the centers had members of non-law enforcement agencies on the governance boards. This lack of involvement led to the assumption that the lack of diversity within the oversight also limited the inclusion of other disciplines. The leadership of fusion centers sets the direction for how information is handled. Of

the directors interviewed, several reported that their leadership understood the need for inclusion of other agencies but did not know how to incorporate them. The members of these leadership teams were worried about a variety of issues that may have an effect on inclusion of other agencies. These issues ranged from security clearances to legal interpretations of the justice system. Examples of the latter pertained to the 28 CFR part 23 and the ability of non-law enforcement personnel to handle documents within a fusion center.

3. A Fusion Center's Funding Stream Impacts the Involvement by Outside Agencies

Most of the centers interviewed are funded by either Law Enforcement Terrorism Prevention and Preparedness (LETPP) grants or State Homeland Security Grant Program (SHSGP) funding. The LETPP grant funds are for explicit use by law enforcement agencies to prevent terrorism. The opinion of most centers is that these funds do not allow the inclusion of other agencies. The SHSGP funds can be used to support all disciplines in the prevention of, preparedness for, response to, and recovery from terrorist acts. However, most of the fusion center funding from these funds is directed to analytical software or building the centers' capabilities.

4. Products Produced by Fusions Centers are Very Generic

Most of the centers are producing and distributing daily or weekly bulletins that are generic in scope. Some of the centers interviewed do build in sector-specific information for the critical infrastructure groups. This information is mostly based on national threat and analysis of impact to local industries. The inclusion of specific details for individual sites was identified by one center. Most fusion centers utilized the Protective Security Advisors (PSA) to work directly with specific sites.

C. SURVEY ANALYSIS

The survey was conducted with responses from emergency management (the highest number of responses), fire service (the second highest number of responses), law enforcement (with an almost equal number of responses), public health, and emergency medical service (with significantly fewer responses). These results were anticipated since most of the sample pool came from or serves in an emergency management capacity. This also was an intentional aspect of participant selection; emergency management serves as the coordinator for all first responder agencies and is seen in most jurisdictions as the center point for information sharing.

The information sharing duties among the respondents varied, with most being centered on homeland security, metropolitan medical response systems, and law enforcement intelligence as the most prevalent. Question # 3 asked for the respondent to specify their role in information sharing. This was the basis for determining to what extent the respondent was involved in information sharing. Question # 4 asked the respondents about their perception of the information sharing among organizations. Forty-five percent of the respondents felt that information sharing only occurred “sometimes when needed.” Twenty-five percent felt that information sharing occurred “low to none, when needed.” The responses suggest a lack of information sharing taking place among those who feel it is important to receive information.

The respondents ranked the importance of components needed for successful information sharing in the following order: multi-agency exercises, multi-agency training, use of technology, Standard Operating Procedures/Standard Operating Guidelines, and governance. This suggests that agencies working together in exercises and training may increase the information-sharing capability and opportunities. Fifty-five percent of the respondents felt that these components were not taking place, which suggest that currently there is a lack of these components.

Respondents were asked about several information-sharing environments and how much they felt those environments were used by their agency to collaborate on information. The different environments were HSIN, FBI/LEO, JTTFs, local fusion centers, and state fusion centers. Of these information-sharing environments, all but local fusion centers were said to be used “only sometimes” as avenues for information sharing. This response may be due to the lack of knowledge on the part of non-law enforcement agency personnel about some of the other environments. These environments might also be seen as law enforcement-only resources that cannot be accessed by other agencies. This response demonstrates the need to better-educate non-law enforcement agencies about the resources available to them. This education should be shared among not only the agencies but also the local and state fusion centers.

Local fusion centers were seen to be used most of the time for obtaining information. This result could stem from the impression that the information is more pertinent to these local agencies because it is being generated on a state or local level. While thirty-one percent of respondents felt that the local fusion center is where their agency gets most of their information from, it appeared that there was a lack of knowledge regarding from where they can get information or if they are getting any information at all.

The survey asked if the respondents felt fusion centers should be required to have participation from non-law enforcement agencies and information sharing networks. Sixty percent said that there would be increased benefit to their agencies in being part of a fusion center that required their participation. This result is not surprising when looked at from the position of the non-law enforcement agencies who feel that they are not being involved in information sharing. Eight-five percent of the respondents felt that a national intelligence and information sharing system should be initiated through a collaborative effort of local, state, and federal governments, as well as including the private sector. This would produce an information-sharing network that involves all sectors of government as well as all disciplines.

When questioned further regarding the development of this type of network, the respondents identified the top three forms of systems that should be built. The highest-ranking solution was an all hazards/all crimes fusion center. Second was information sharing networks where all disciplines have access and are only limited by their roles and clearances. Third was the use of terrorism liaison officers and fusion center liaison officers who work with the agencies. Along with this question, the respondents were asked “what is the most effective means of sharing information with trusted individuals of non-law enforcement agencies?” The overwhelming response was for the building of Virtual Private Networks (VPNs) to access information sharing.

These results point to several gaps in the information sharing community. These gaps seem to be a lack of information being made available to non-law enforcement agencies on avenues to get information, a consolidated effort by fusion centers to get these agencies involved, the need for specific intelligence briefs for different requirements of agencies, and the need for better technology usage to facilitate information sharing. There is also a clear need to promote educational opportunities regarding existing systems and to work to establish new networks. Throughout the survey and interviews, it was apparent that this issue of information sharing is very complicated and has many parts.

THIS PAGE INTENTIONALLY LEFT BLANK

V. COMPONENTS OF A SUCCESSFUL INFORMATION SHARING SYSTEM

The answers to the research questions addressed by this thesis have been grouped by two areas. The first includes those things that are driven by or require the humans involved to posses or create attitudes that are conducive to success. This area will carry the most weight in the recommendations presented in this chapter, since many of the responses were influenced by participants "being allowed" or "being asked or invited to participate." This sense that the human control of whether or not information is shared is based on a human decision is why many in the non-law enforcement agencies feel they are not getting the needed information.

The second answer to the research questions focuses on the technical aspects that will allow the sharing of information as long as the first part–the human element–is willing to allow it to take place. The technical aspects include the components that are currently available as well as suggest further research into future development of systems.

The questions that drove this research project were the following.

- What are the human components that are necessary for successful data and information sharing between the law enforcement community and those non-law enforcement public agencies and private sector partners?
- How do we structure a system to enable these human components to allow data and information sharing while at the same time providing the necessary critical information protection?
- How can fusion centers leverage the technical components such as technology, standard operating procedures, and interoperable systems to enhance data\information sharing? Specifically, how can various pieces of information that are brought together through different technologies, provide interagency and private partners with real time personalized intelligence?

The recommendations made in answer to these questions can be broken down into two areas, as stated previously, the human element and technical

requirements. Each of these two areas will be addressed with components that will give an outline of the steps and necessary pieces that must be put together to complete the full model. The first research question looks at the overall need for components of information sharing which cross the both analysis areas. Some areas will be addressed in the human side of the equation while the technical components are addressed by looking at current standards, technology as well as future developments in these fields.

A. MEASURING SUCCESS

There can be many necessary components for a successful system of any type. These can be found in numerous business models that are as different as the companies and leaders who built them. Through the years, many large businesses have changed their business models as the economy, technology, work force, and the consumer have changed. One of the things that have made many companies successful over time is their ability to be flexible and allow for change to take place. Companies that have been successful for several decades are good examples of these who have been flexible in their business model. Companies such as IBM, Procter and Gamble, Sears & Roebuck, and 3M are example of these types of companies.

The United States government uses models to create success when developing new or modified plans. For example, the DHS Tactical Interoperable Communications Plan was used to help urban areas develop some of the components of their radio interoperability plan into manageable sections. Models are used to guide the development of an anticipated pattern to achieve consistent results. Although the results may be slightly different based on the factors used to form sections of a plan, the overall product at the end should be able to be compared against other programs.

What does success look like? How do we know when we are successful in a project or program? Success can be defined as achieving one’s goal reaching the point at which a level of completeness has been obtained and the desired

outcome has been accomplished. For information sharing networks, success will vary based on the strategic vision. If the goal is to have the ability to call the members of certain agencies and tell them important information, then success may look like a phone tree that is accurate and updated regularly. If the vision is to have a network approach that automatically passes information to a group, a system of systems will be needed. The achievement of success will be reached when the strategic vision is able to be completed without additional input or change. Describing success is sometimes difficult, but the desired level of success must be able to be communicated to all those involved for a shared understanding.

When conducting the interviews and research for this thesis, participants were asked what they thought success meant to them. All of the respondents saw success as the point at which their fusions centers would be able to provide all of their partners the information that they had received and analyzed in a format that was beneficial to each agency's individual needs. This description is broad in scope but narrow in understanding.

The needs of each partner are different based on the discipline and request for information needs. The local partners look for information that is specific to their jurisdiction and has relevance to an action item or being made aware of specific situations. These partners will measure success based on how quickly information is passed to them and in what form they receive it. This can be one of the most challenging aspects of success for a fusion center. Many times partners will not understand the time lag that may occur in delivery of their products.

A shared understanding by all partners of the process of information analysis is key in shaping their views of success. Having a product of analysis that is useful is another key measure of success for the local partner. A blanket product, sent to all partners from the fusion center that does not provide specifics for their agencies is of lesser value than pertinent information that helps individual agencies make decisions. Local partners will be the biggest critics of

the fusion center's operations and must be heavily involved in the development of success benchmarks. These benchmarks will guide the fusion center in identifying what the fusion center products should contain and look like.

The staff and management of the center will also evaluate success for the fusion center. Processes that are difficult to perform may not achieve the desired results and may have a negative impact on what success looks like. This is an important reason that staff as well as management must work together to build systems that compliment the needs of those who must use them. Several of those interviewed commented on the need for better coordination between the systems and their human interfaces. While few of those interviewed said this was a current issue in their center, it was identified as a potential problem as the fusion center looked to expand to include new partners or products. For this reason, it is important that steps to increase information sharing must be thought out and mapped to achieve a successful outcome. The strategic view of the information-sharing network should be evaluated and adjusted regularly to see if success is possible in the current plan.

B. THE HUMAN ELEMENT

1. Governance

The need for oversight and direction is a cornerstone of the development of any organization. The proper organization that represents all parties involved is a critical part of a successful program. Some urban areas have a formalized and established governance structures for their UASI grant programs, which includes the first responders and public safety organizations within the geographic area. Many of these demonstrate a higher level of proficiency in managing the UASI programs than those who have limited diversity in their makeup. This proficiency may be, in part, a result of the larger, more seamless shared systems that more closely correlate with an established regional

governance structure. This correlation is based on areas with shared systems must have developed and adopted consensus requirements, funding strategies, and longer term agreements to support their systems.

Governance refers to the establishment of a shared vision that creates an effective organizational structure that supports any project or initiative that seeks to solve issues. This effective organizational structure provides guidance and support through common policies, processes, and procedures. By establishing a common governance structure communication, coordination, and cooperation will be increased across the agencies and disciplines that are working to achieve an acceptable level of information sharing capability.

The members of the governance group should consist of representatives from all entities of the pertinent public safety disciplines within the identified region. Members of the governance group should be representative of all first responders, plus emergency management and public information (media relations is important in a terrorism incident). The group should include the appropriate state and federal agency representation such as state police, FBI, Secret Service, etc. There may be a need to include key leaders of other city-county agencies with certain authorities such as budget and management control. The group should be representative of all jurisdictions that would be considered for a request for information or be asked to help in any fashion.

A formal governance structure is critical to the success of any information sharing system success. A major advantage will be the involvement of the high-level administrators of the jurisdictional agencies. If each agency involved is required to have participation by the top-level administrator, more equality can be brought to the effort.

The governance structure should be based upon a written agreement, among all participating agencies and organizations, which provides responsibility and accountability. This written agreement–which can be either a Memorandum of Agreement or a Memorandum of Understanding–should be reviewed by legal

counsel for all signatories.[34] An analogy for the MOA is to think of it as outlining what would be included in a contract statement of work. You'll find the documents referred to in multiple and contradictory ways as to their use for financial purposes. Your command may have published guidance that specifies which term to use for which purpose, or your legal counsel may have specified a procedure to use in your case. Your best option is to see what your command is currently doing and follow the established practice.[35] Specific responsibilities and rights of the participating agencies and disciplines must be clearly defined. The written agreement should address, among other issues the following.

- Providing assets to the system
- Using the assets of the system
- Management of the assets
- Problem identification and resolution
- Funding requirements of participating agencies
- Expectations of the agencies
- Procedures for agencies to cease participation in the system

The governance should identify the need and makeup of two important groups–operational and technical–that will help to identify and resolve issues as they arise. These two groups would report to and take direction from the Governance Board. The two groups would represent both the technological and human aspects of the system.

a. Working Groups

The Operational Working Group would be responsible for determining the operational requirements, developing standard operating procedures (SOPs), and coordination of training. This group could also review

[34] These titles are interchangeable and the use of the term Agreement or Understanding have, in general, no special significance. In practice, the MOU is often viewed as an overarching document outlining goals, etc., while the MOA can be thought of as an implementing document.

[35] AT&L Knowledge Sharing System, Ask a Professor–Question & Answer Detail, Business, Cost Financial Management, https://akss.dau.mil/askaprof-akss/qdetail2.aspx?cgiSubjectAreaID=15&cgiQuestionID=20023.

existing SOPs (and apply these as appropriate to anticipated incidents), develop formal written guidelines and checklists for Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) and all-hazard events, and ensure that SOPs and checklists follow ICS/NIMS standards.

The Operational Working Group will have to coordinate and work with the second group, the Technical Working Group. This group's focus would be on the technology aspects of the system and how systems work together. This would include identifying existing technical solutions (including appropriate and available equipment that can be used to handle data sharing) and evaluating alternative solutions with regard to potential problems between software and hardware. The Operational Working Group should work to identify the most appropriate solutions that will still accomplish the goals set forth by the Technical Working Group. This cohesion of work between the two groups is important to ensure that all requirements are met. These solutions may be evaluated by exercises or virtual testing to ensure appropriateness for the application in the field.

b. Legal Considerations

Legal issues that pertain to the transfer of information are an important part of the governance of information sharing. Many fusion centers enlist the participant of legal counsel to help craft and review all aspects of the oversight of the operations. Legal counsel will need to be involved in the development of the MOA/MOUs to ensure jurisdictional authority is followed. In addition, any rulings that have precedence on sharing of data should be reviewed to help in the development of the network.

The participation by legal counsel that is educated in fusion center and information technology is important. Fusion center management must select the appropriate legal counsel to participate in the governance structure. Many of those who participated in the interviews stated that they had to work through several different attorneys to get those with the specialties needed during

development. No one attorney will posses all of the knowledge necessary to address the varying aspects of information collection, storage, dissemination, and technology components. As part of the governance structure, the legal counsel should have freedom and authority to participate in all discussions pertaining to the information-sharing network's design and operations.

2. Relationships

To achieve success, the information-sharing network will need to identify those partners that have an interest in the system. To help identify those partners, the mapping of potential participants from the onset will help to ensure a comprehensive list is developed. The direction and scope of the network will determine the size and makeup of the participants. A law enforcement-only network may be confined to those agencies who are credentialed as law enforcement or that serve law enforcement needs. Those networks that will include non-law enforcement agencies will need to do extensive mapping to see what agencies or disciplines will have information needs and can provide information to the network. These agencies or disciplines may need to be evaluated to define the extent of their participation as well. Some will be full partners in the network with decision-making authority while others may be only receptors of information.

Participation by agencies or disciplines will be dependent on building on existing relationships or developing new ones. Relationships are based on understanding the needs of others as well as one's own needs. Relationships with information-sharing partners are very similar to personal relationships. The network must be able to recognize or understand the needs of all those involved with the network in order to be successful.

Building upon existing relationships is an important factor in information sharing. Many times informal connections between individual members of different agencies are used to help solve problems or to get information. The information-sharing network will need to establish formal intra-agency

relationships rather relying on informal individual relationships. Existing connections may be used to open doors and pave the path for development of the agency relationships. Deepening the relationship between agencies produces additional personal contacts that may be utilized later in new ways.

Agency relationships should be built on consistent practices utilized by all members of each agency. How many times have two information requests generated a different answer from the same agency? This creates disparities in agency relationships and can cause degradation in the relationship. When there is no existing relationship with an agency, one must be built. This will require a variety of exercises in order to establish the groundwork for a healthy relationship. These exercises should include researching the needs of new agency partners and creating a clear understanding of what each agency does. Many of the fusion center interviewees expressed some knowledge of what other, non-participating agencies need, but did not fully understand what the fusion center could do additionally for these agencies. By interviewing the new partner and developing a better understanding of operations and systems, gaps in information may be identified that will facilitate a new relationship.

3. Megacommunities

The building of larger relationship groups can be compared to building a community–a larger group that exists to provide benefit to individuals. In the book *Megacommunity,* the authors explain that there is a new way of solving problems that are common to multiple people or organizations. The approach spans business, the government, and the communities we live in to address shared commonalities. By looking across these different yet connected groups we see that each can support the other in solving a vast array of complex issues. These new complexities are a natural consequence of a world made smaller by greater integration and interdependency. Issues that arise in this environment can abruptly and unpredictably escalate, with a scale and magnitude that can quickly overwhelm the effected institutions. As a result, leaders from all three sectors of

the Megacommunity face a growing need to operate in a more open, distributed and collective manner that recognizes the shared nature of risks, rewards, and responsibility. Unfortunately, this type of activity is not intuitive for most leaders.[36]

This view of interconnectivity has important implications for the information-sharing environment. The need to understand how each individual relationship is tied together in a Megacommunity with other relationships is important. As important is the fact that individual relationships within the Megacommunity will overlap. The power of the Megacommunity begins to take shape as we perform a link analysis of who we need to share information with and, in turn, who those groups or individuals need to share information with. What starts to happen is a network of groups begins to build that has no direct ties but is loosely connected through the Megacommunity.

For example, the incorporation of private sector members in the information-sharing network produces a very short list of possible candidates that would be considered by most law enforcement-centric networks. When those few members are included and then look at who they need to share information with, a more free-flowing network begins to develop. It is likely that the third and fourth layer of contacts that a private sector partner might have could be the contacts that other private sector partners have as well. This loose connection might not be identified unless a Megacommunity is established and mapped out.

The effects of not knowing those connections could be seen during Hurricane Katrina. Many public and private sector agencies relied on the same supply chains for many of the goods and services needed in the first few days of the disaster. As a result, many issues arose from not having enough sources to deliver or distribute the needed goods. The Megacommunity concept of info sharing allows agencies to identify those connections and use the strengths of each connection to strengthen the community as a whole.

---

[36] Mark Gerencser, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly, *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together* (New York: Palgrave Macmillan, March 2008), 9.

4. Trust

What is the basis of a relationship that enables individuals to share important information? How does one know that information shared is kept to only those individuals who should have it?. There is one thing common to every individual, relationship, team, family, organization, nation, economy, and civilization throughout the world–one thing which, if removed, will destroy the most powerful government, the most successful business, the most thriving economy, the most influential leadership, the greatest friendship, the strongest character, the deepest love. On the other hand, if developed and leveraged, that one thing has the potential to create unparalleled success and prosperity in every dimension of life. Yet it is the least understood, most neglected, and most underestimated currency of our time. That one thing is trust.[37]

In the information-sharing network a level of trust must be established before a relationship can be built. A Megacommunity depends on relationships, and the basis for connections to within this network is trust. Those in the information-sharing network must understand that there are several types of trust that have to be identified. In his book, *The Speed of Trust*, Stephen Covey writes that there are five waves of trust: self trust, relationship trust, organizational trust, market trust, and social trust. This trust model serves as a metaphor for how trust operates in our lives. It begins with each of us personally, continues into our relationships, expands into our organizations, extends into our marketplace relationships and encompasses our global society at large. This reflects the strength of the “inside-out” approach: to build trust with others, we must first start with ourselves.[38]

A successful information-sharing network needs to be able to pass information to others and get information from others. How do we build the trust necessary to allow this to happen? We have all heard the saying “it is better to

[37] Stephen M. R. Covey, *The Speed of Trust. The One Thing That Changes Everything* (New York: Free Press, 2006), 1.

[38] Ibid., 41.

give then receive" and "the best way to build trust is to give it." In today's law enforcement-centric information, sharing environments there seems to be a reluctance to take the first step in giving trust. In many fusion centers, the sharing of information outside of the center is questioned in terms of safety and security. What if the trust existed between those agencies and personnel within the fusion centers with agencies and personnel outside the center? The difference of having an existing relationship among the Megacommunity built on trust of the individuals, trust in the organization, trust in the technology used, and trust in the society of those members would be a powerful tool. The power of trust drives every decision made about sharing information in today's world. From private corporations worried about competition to fusion centers concerned about information getting into the hands of the enemy. There exist barriers many times in getting the information to those who need it, in a timely and accurate fashion. Many times these barriers are based on a lack of trust. This is the basis of relationships and why it is important to establish the trust on the five layers. How can we build a system of establishing trust between agencies and individuals that opens the barriers and allows for information sharing to take place without hesitation or reluctance? There are ways to create individual trust through relationships but what is needed is more standardized organizational trust. Too many times in the information sharing community, we are comfortable with certain individuals but not the agency as a whole. What happens to the information sharing when that person is not available or leaves the organization? Does the information still get passed to the necessary end point? Effective information sharing relies on trust and the trust in the Megacommunity that the center is part of. Our goal should be to establish organizational trust where individuals serve mostly as the human end points. The trust should lie within the connections of the Megacommunity and its agency members. Systems should be built that provide the security that supports the trust factor between members.

There should also be methods in place to ensure the trust is not abused or broken. Through collective views of what trust is and how to protect it, all members will understand the importance of keeping it.

5. Leadership

The leadership of the member agencies of the information-sharing network will be an important component of the structure. As discussed earlier in this chapter, the governance of the network is a key component and that governance starts at the top executive level of the organization. However, leadership is a component that exists at all levels of the organization and can be found many times within informal ties. Leaders are those people with vision and the courage to reach for their vision. Many times the leadership necessary for an organization to grow or change will come from those closest to the problem. Creative leadership is necessary in the information-sharing network to allow those providing the services the empowerment to provide the organization what it needs to be successful.

Effective leadership will be based on the importance of the network–not the individuals–to be successful. This leadership must insure that the following questions are answered at the lowest level; what are we accountable for, how will we do it, and how will we know when we have done it? While governance will set policies and overall direction of the organization, leaders will be the ones rowing the boat and pushing it forward. The leadership of the information-sharing network will be also need the ability to change those things that need to be changed. An understanding of the systems and the personnel will provide the best gauge of success for the leaders. This can only come from being an integral part of the daily process of the information-sharing network. Mid-level management is often entrenched in the processes that provide first-hand leadership decisions that make the organization function.

In the book *Edgewalkers,* the author Judi Neal talks about those people who can walk between two or more worlds and relate the two together. She describes those leaders who bring together organizations or people who can forge alliances and create unusual opportunities, and the abilities that are essential for innovation and growth.[39] Leaders of information sharing networks will have to be able to walk the edge between their own agencies and those outside agencies they need to work with. Having the skills to do so will provide opportunities for success that cannot be written in a procedure manual or built into a technology. The leaders of the information-sharing network, at whichever level of management they are within their agency, will be critical to the success of the larger organization.

C. THE TECHNICAL CHALLENGES

The challenges to information sharing are (1) the ability to get people information when they need it and (2) the ability to use the information received. Many of the research respondents spoke of the need to incorporate multiple feeds of information into a global view of what is happening. As we look to exchange more data in different formats, we must identify the technology that will support the exchange. With technical requirements come human interface. This interface requires the determination of how the technology will be used, by whom the technology will be used, and the parameters within which it will be used. All of these are questions that must be identified and agreed upon first by those at the highest levels, then down through management of all agencies involved so that systems can be built to support the requirements. The following components were identified by the respondents as important to building successful technical systems: interoperability, standards, and the technology itself.

[39] Judi Neal, *Edgewalkers: People and Organizations That Take Risks, Build Bridges, and Break New Ground* Annotated ed. (Westport: Praeger Publishers, October 30, 2006), 25.

1. Interoperability

Interoperability refers to the ability of diverse systems and organizations to work together (inter-operate). The term is often used in a technical systems/engineering sense, or alternatively in a broad sense, taking into account social, political, and organizational factors that impact system-to-system performance.[40] In the case of information-sharing systems, the need to have systems that are interoperable is a high value concept that must be implemented throughout the system. The core aspects of the system must be built around the ability to work with like systems as well as other systems that may provide value. Other systems might be in the form of data sets from other programs or systems that analyze the data held with the primary system itself.[41]

With respect to software, the term interoperability is used to describe the capability of different programs to exchange data via a common set of exchange formats, to read and write the same file formats, and to use the same protocols. (The ability to execute the same binary code on different processor platforms is 'not' contemplated by the definition of interoperability.) The lack of interoperability can be a consequence of a lack of attention to standardization during the design of a program. Indeed, interoperability is not taken for granted in the non-standards-based portion of the computing world.[42] As traditional boundaries between institutions and disciplines begin to blur, the need to access information from a wide range of sources increases. This will be both from within and outside of specific subject areas. In many cases, both goals and problems are similar, and there is much to be gained through adopting common solutions wherever feasible.

---

[40] Wikipedia, http://en.wikipedia.org/wiki/Interoperability.

[41] Ibid.

[42] Ibid.

Being seen to be interoperable is becoming increasingly important to a wide range of organizations. The need for information sharing systems to be interoperable in their administrative systems as well as the technology is one of the underpinnings of the framework for success. With standards such as Global XML the design of systems is becoming more interoperable to support open architecture components. The availability to access and use valuable information that is being made available to a wide range of users, often for the first time by interoperable systems will enhance the all parties capabilities. In some cases, this new openness is in response to a requirement for accountability to the stakeholders in order to make good business decisions in order to harness and use knowledge.

The drive towards interoperability will lead to changes in the way the organization operates in other aspects as well. A change in the way an agency views other agencies, once they have agreed upon terms for one aspect of their joint operations, will lead to new and more positive opportunities to work jointly. A truly interoperable organization is able to maximize their value to themselves with internal systems but also make themselves more valuable to outside systems. Once an agency is able to exchange their information effectively with other equally interoperable bodies, new knowledge will be generated from the relationship between these previously unrelated sets of data. When agencies change internal systems and practices to make them interoperable with other systems, benefits for all the organizations as well as those making use of information that is produced cannot be measured.

2. Standards

Standards establish a commonality for operating at certain levels or to a specified capability. A technical standard is an established norm or requirement. It is usually a formal document that establishes uniform engineering or technical criteria, methods, processes, and practices.[43] Standards are the benchmarks for

[43] Wikipedia, http://en.wikipedia.org/wiki/Standard.

a process that controls the way things will be done. Many of the components of an information-sharing network will need to be addressed by standards. These could include hardware and software standards that must be met for systems to operate properly. Standards may relate to the components within the information-sharing network that are controllable or those components that you must build the network around that are not controllable. Issues like bandwidth of network connections may not be able to be changed so the system you build will have to be adjusted to meet the fixed standard of service. Each component of the information-sharing network will need to be reviewed for pertinent standards and their interdependencies within the entire network.

3. Technology

The use of technology will be one of the most important components to a successful information sharing network. Technology is responsible for many changes seen in the field of information sharing to date. As the effects of the attacks on 9/11 demonstrated, agencies and organizations are not talking to each other. While many pointed fingers at the federal government for not sharing information about threats and warnings, state and local levels of government took part in the failure that continues today. How many agencies share their data with other agencies within the same discipline? How many agencies share data with other disciplines? Many people have no idea on who can get the data or how they would get it if requested to.

Technology provides connections between people and systems that humans alone might not be able to accomplish. Technology can conduct analyses of information that would take humans hundreds of times longer, if at all possible. Understanding the needs of the information-sharing network requires identifying the types of information to be shared as well as the tools used to do so.

Many agencies have organizational drivers, which direct the behavior of the organization. Some agencies use multiple technologies in their daily operations while some use very few. The access an agency has to technology will determine its ability to share information. Those members of the information-sharing network that use very limited technology will be challenged in their ability to participate in the initial stages of the network and thus may be more reluctant to participate. In contrast, those agencies that have invested in many types of technology will be more accepting of participating in information transfer due to their knowledge and familiarity of the benefits technology can bring. This will also provide opportunities to research and invest in new technologies specific to the information-sharing network.

Shared technology will necessitate discussions on information assurance and computer security issues. The type of information sharing will be dependent on the type of technology being used. As our society has become more dependent on technology, the increase in security of the information within that technology has increased. Many forms of interagency information sharing may be complicated by increased security measures. Some of these security issues may be addressed through standard operating procedures. Others will need specific attention and will drive what information is available to be shared and how it can be shared. Legal and authoritative regulations will need to be evaluated, to ensure technology systems do not violate any laws or policies. While this thesis does not cover the types of technologies that should be utilized it is important to understand that information sharing networks must share? some form of technology to be successful.

4. Standard Operating Procedures

In the information-sharing environment, there will need to be managerial authority on how things are done and by whom. The use of standard operating procedures (SOPs), are important to ensure that personnel and member agencies have reached agreement on the processes. Standard operating

procedures can be considered formal rules and regulations that are a necessary part of the process of any organization to provide guidance for those expected to perform duties or functions. Without standard operating procedures, chaos would reign and no process would evolve. SOPs also communicate to members what is expected of their performance and eliminate any surprises for the members.

Members of the information-sharing network may be individuals or agencies. The organization needs the SOPs to explain what each member's responsibilities are and how they support other members. All members mentioned in the SOPs need to have the opportunity to participate in the development of the SOPs as well as comment on changes. Through participation in the process, member agencies have the opportunity to input their requirements as well as bring attention to inabilities they may have to fulfill request by other agencies. The development of SOPs for an information-sharing network is not a singular event. It will take many attempts to address all of the issues that will have to be identified and decided on.

In addition, there will need to be revisions to these procedures when new members are identified or technology changes warrant new processes. SOPs must be specific to the mission and scope of the information-sharing network. Each procedure will need to address a section or part of the operation and not attempt to be too large in scale. The more finite a procedure, the easier it can be adopted and implemented. The need to ensure procedures do not conflict will be an important step in the development phase. An overall view must be taken at all times to provide a careful analysis of the cohesion of procedures. Standard Operating Procedures are meant to contribute to the effectiveness of the functions an organization conducts. They should not become barriers to success nor should they exclude individual exceptions when necessary. The success of the information-sharing network will rely on processes that include automation and the reliability that will come from these procedures.

5. Integrated Technologies

The second part of the research question asked how to provide real-time personalized intelligence. The vision of an integrated information-sharing platform between multiple agencies and multiple disciplines has long been seen as unreachable. Today, a new wave of technology allows for integration of data into a useable format. As we work to become more inclusive in our preparation, prevention, response and recovery from events, we must look at those processes that will allow for better communication systems.

The goal of any information system is to get information to those who need the information to enable them to make the most informed decisions possible. Critical information from as many sources as possible is imperative when evaluating a decision that affects different agencies. The sharing of information in a real-time environment can be accomplished using integrated systems. The following is a representation of how this system would share information through secured portal access. The diagram shows the varied points of data collection and storage that represent the multi-agency aspect that information should include.

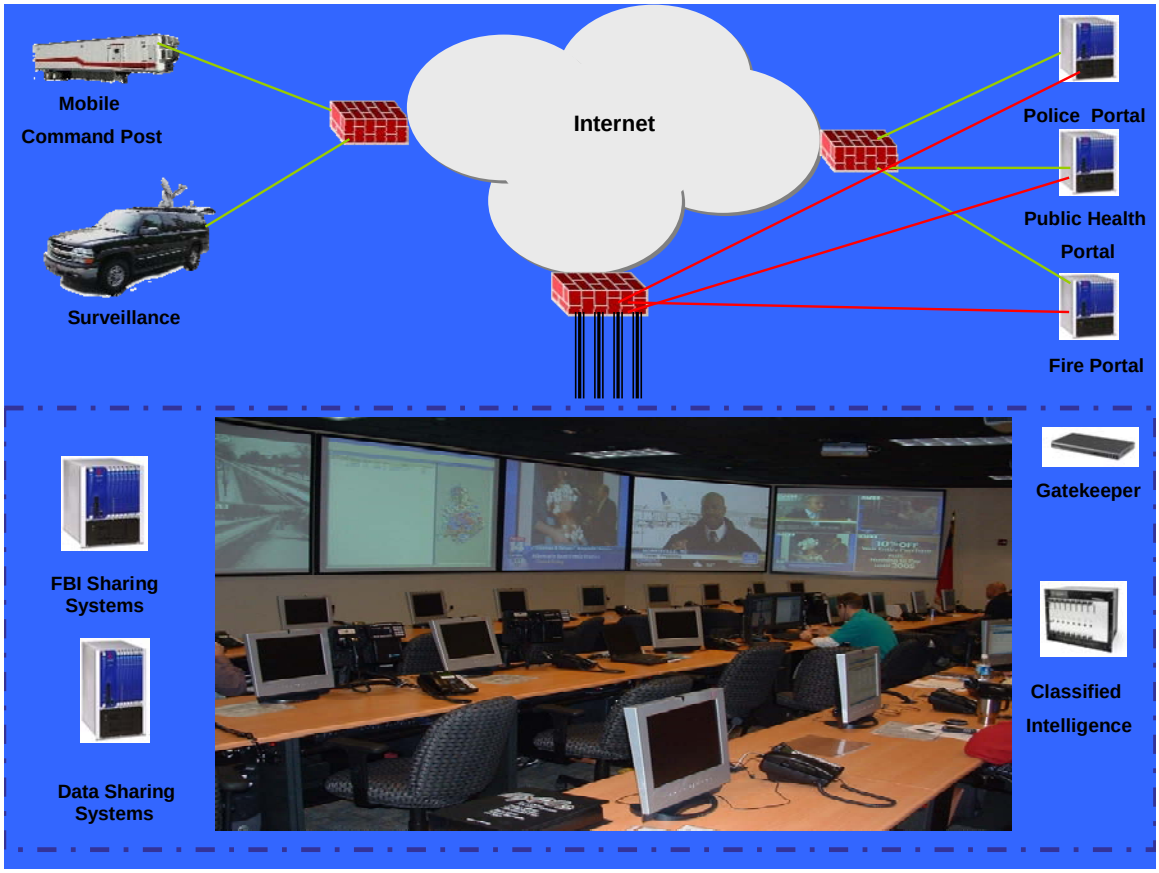

Figure 1. Integrated information-sharing Systems

The challenging portion of this concept will be the transmittal of data, photos and live feeds from locations such as the fusion centers and emergency operations centers to field units. This will provide two-way interaction with commanders in control centers as well as provide information to decision makers on the scene. The goal here is to provide as much additional information as possible to all units responding to an incident while ensuring that all receive the same information. The ability to link backwards with information from the scene will also be needed for oversight.

This portion of the project could be addressed using mobile data computers (MDCs) and commercial connectivity mediums. While MDCs are not a new technology, their use in the first responder community as “smart terminals’ is relatively new. Agencies are still looking for the best combination of technologies

that will provide the highest level of connectivity, bandwidth, security, and at a reasonable cost. As agencies work to push more data and larger images, current systems are restricted by bandwidth availability and the costs to provide a dedicated system. New products like WiMAX are providing some promising alternatives.[44] The goal is to incorporate this new technology into daily activities. This will benefit the investment and provide stability to both the system and the users while increasing their confidence in the system. While providing high-speed data transfer of information we also must look at the security of these systems and the ease of use by everyday first responders. The benefit of real-time information is the ability to make decisions while monitoring the outcome of previous decisions. As new linkages to other data bases or sources of information are discovered agencies will be able to take advantage of each other's systems. This is an example of how technology is changing the way certain duties are performed; such technology must be incorporated with strong vision and planning.

6. Protecting the Flow of Critical Information

The second part of the first research questions relates to the protection of critical information through development of a structured system that will allow for the sharing of the information in a timely manner. The use of existing systems such as Constellation/Automated Critical Asset Management Systems (C/ACAMS) a Web-enabled information services portal that helps state and local governments build critical infrastructure/key resource (CIKR) protection programs in their local jurisdictions. C/ACAMS provides a set of tools and resources that help law enforcement, public safety and emergency response personnel.

[44] WiMAX, http://www.wimax.com/education. WiMAX is a wireless digital communications system, also known as IEEE 802.16, that is intended for wireless "metropolitan area networks." WiMAX can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3–10 miles (5–15 km) for mobile stations. In contrast, the WiFi/802.11 wireless local area network standard is limited in most cases to only 100–300 feet (30–100m).

- Collect and use CIKR asset data
- Assess CIKR asset vulnerabilities
- Develop all-hazards incident response and recovery plans
- Build public-private partnerships

Using C/ACAMS also provides state and local jurisdictions with a practical way to implement the National Infrastructure Protection Plan (NIPP), including the NIPP Risk Management Framework.[45] C/ACAMS provides a vetted process by which information can be securely shared with the human element interference once members of the community are approved. This also will allow the exchange to law enforcement agencies form those agencies outside including the Private Sector. The C/ACAMS program also uses the Protected Critical Infrastructure Information (PCII) Program to implement protective measures for accidental or intentional release of information. The Protected Critical Infrastructure Information (PCII) Program is an information-protection program that enhances information sharing between the private sector and the government. The Department of Homeland Security and other federal, state and local analysts use PCII to for the following.

- Analyze and secure critical infrastructure and protected systems
- Identify vulnerabilities and develop risk assessments
- Enhance recovery preparedness measures

If the information submitted satisfies the requirements of the Critical Information Act of 2002, it is protected from the following.

- The Freedom of Information Act (FOIA)
- State and Local disclosure laws
- Use in civil litigation

Protected Critical Infrastructure Information cannot be used for regulatory purposes and can only be accessed in accordance with strict safeguarding and handling requirements. Submissions that do not meet the requirements are

[45] United States Department of Homeland Security, *National Infrastructure Protection Plan*, *Constellation/Automated Critical Asset Management System*, http://www.dhs.gov/xinfoshare/programs/gc_1190729724456.shtm.

destroyed or returned to the submitter. The PCII program allows both law enforcement and non-law enforcement personnel to have access to this important information. Protected Critical Infrastructure Information (PCII) may be accessed by federal, state or local government employees and their contractors who meet the requirements of the PCII Program standard access policy. Before accessing PCII, federal, state or local government employees or contractors must have the following.

- Complete training on the proper handling and safeguarding of PCII
- Have homeland security responsibilities
- Have a need-to-know the specific information
- Sign a non-disclosure agreement (non-federal employees only)
- Be certified by the PCII Program Manager or PCII Officer (contractors only)

The PCII Officer manages the PCII program in an accredited entity and ensures that all PCII received is used, safeguarded, stored and disseminated in accordance with specific procedures. Accredited entities must have a PCII Officer.[46]

These are two examples of systems that allow users to share information in a secured and protected environment that exists today. The use of these tools can be greatly enhanced with future additions to the programs. One avenue that is being explored is the integration of the DHS Buffer Zone Protection Plan (BZPP) Program which is working with C/ACAMS to incorporate the information from both programs into one web portal. This will allow real time sharing of the information for both planning as well as in the response mode for first responders. The management of the security of information sharing programs is a necessary part of the program and must be controlled. The important aspect is to build the systems to encourage the human element to allow access to the systems through the components identified earlier in the chapter.

---

[46] United States Department of Homeland Security, *National Infrastructure Protection Plan. Protected Critical Infrastructure Information Program*, http://www.dhs.gov/xinfoshare/programs/gc_1193089801658.shtm.

D. CONCLUSION

While the identified components represent a vast majority of the areas needed to build a successful network, it is recognized that there may be others that were not mentioned. In addition, many sub-components within each of the mentioned sections upon could be explored and expanded upon. To be successful at information sharing, we must look at a wide array of both human and mechanical components. These components all build upon each other and are interdependent on accomplishments of previous successes. Through evaluation of the components and how successfully we implement each of them, we can determine the likelihood of overall success of the network.

Developing strong relationships between the law enforcement community and the non-law enforcement agencies must be the first priority. In past years the segregation of these two groups in the information sharing environment has caused distrust and a lack of agreement between the two. To build an information-sharing model that works, we must establish the base, which will support all of the challenges and hurdles that will be encountered. The human element represents those things that can be controlled by human interaction. These components are those that can and will have to be controlled by administrators, chief officers, elected officials, and the other top-level managers. To be effective, a top-level official has to support the components both internally as well as externally, through demonstration of their willingness to work with other agencies as well as work within their own organization to establish and support these components. There may be some resistance from members of agencies as to the value or ability to support this development. This is the linchpin of the administrator's support and backing. If the top-level person truly values the components then the organization must follow.

When other administrators see their peers promoting these components then they will feel compelled to do the same. Leadership is a component that is needed to set the example and reach across the aisle to other organizations and ask them in. Showing leadership qualities will impress not only the members of

outside agencies but also may instill confidence within the administrators own organization. Governance and megacommunities will be the last to be built, once the other components are established. The governance structure cannot be built until the relationships and trust between the agency representatives has been built. People hesitate to reveal their weaknesses until they can trust they will not be taken advantage of. The governance of the information-sharing network will need to be representative of all the agencies and disciplines that are part of the Megacommunity.

Once the first layer of the system is built on a strong foundation, the technical challenges can begin to be addressed. These components are ones that will need buy-in and support from the human element. Through components such as standards and interoperability, the technology can be utilized to build the system. Standards will give the outline of what is to be accomplished. Is the goal to have voice and data transfer; is there a need for video teleconferencing, or are there security issues and clearances that need to be addressed? The standards or even some federal laws will have to be addressed and followed to insure acceptance.

The need is to establish and build interoperable systems to join other networks or systems and grow the capabilities even further. By using open architecture and standards-based networks, the ability to share the information will face fewer challenges than a non-conformant system. Once the standards and interoperable goals have been identified, the right technology can then be employed to address the needs. The system may require some research and development to adjust the technology to meet the specific needs but by having a solid support in standards and interoperability the development will be made much easier.

The human element will make decisions on the technical elements much simpler and more focused on the needs of all parties. This will allow the system to be built with input and support from the megacommunities' perspective rather than a single point of view. Through the development of an information sharing

system using this model, the potential for success will be much higher. This in turn will result in a greater opportunity for true collaboration between the agencies involved and will produce true benefits and results.

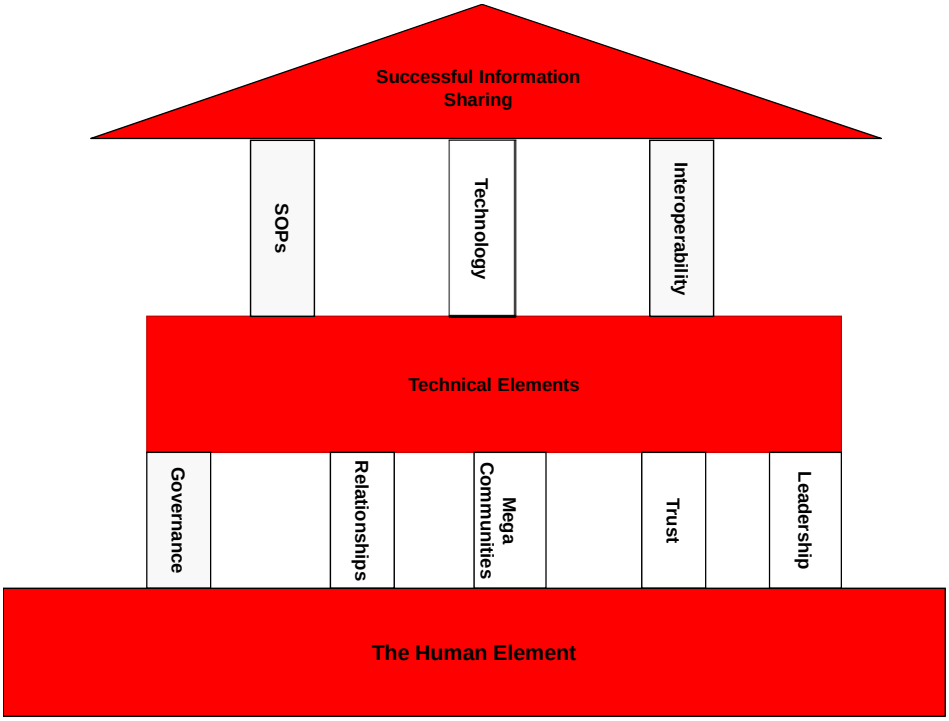

Figure 2. Information Sharing Component Model

The information sharing component model illustrates the need for a strong base of human interaction to establish the foundation to build a system of technical support. The pillars of Governance, Relationships, Megacommunities, Trust, and Leadership support the interaction that members of the information sharing community must have to facilitate the exchange of data. The responsibility of the top leadership of agencies involved in Homeland Security Information Sharing must be understanding and responsive to the need for inter-agency human interaction.

The pillars built on the Technical Elements are those components that actually move the information between the agencies. This can only be built and supported once the human elements are established. The Standard Operating

Procedures, the Technology, and the Interoperability of all components support the system of information sharing with relying on the human decision making nor the discrimination between agencies or disciplines that might occur without the base of human interaction.

Through this model, a robust and inclusive system can be built that includes all agencies and disciplines that are part and need to be a part of the information sharing community. While there may always be a need for refinement base on the exact system be built, the basic consideration that the interaction between agencies and disciplines must first be refined and built on a solid foundation before any other parts of the system can be established.

VI. CONCLUSION

There are those within the information-sharing network who feel the ideas and suggestions identified here are not feasible. In fact, some may feel that these new networks might be counterproductive to agencies like law enforcement and federal agencies, whose true goal is criminal investigations within fusion centers. This feeling might be from a fear of decentralization and the possible dilution of the information. The people who currently run or operate fusion centers often look upon any changes as potential breaches in security for their operations. The FBI is the lead agency for intelligence gathering and terrorism information sharing within the United States. The establishment of Joint Terrorism Task Forces JTTFs was an attempt to include state and local law enforcement in the information sharing and investigative aspects of their operations.

Most JTTFs are 100 percent law enforcement-based, which promotes the inclusion of only those agencies in their information sharing networks. The inclusion of the other agencies from non-law enforcement disciplines identified in this thesis may help to open up some doors for sharing of information. While there may still be some areas that are not fully engaged, implementation of these new partners and systems will enhance the productivity of information-sharing networks and involvement on the part of all agencies. From the research, it was found that there is a reluctance to include new partners in the information-sharing systems for one or more of the following reasons.

- Non-law enforcement agencies cannot provide any valuable information about investigations or indicators of acts of terrorism or other crimes
- These new non-law enforcement agencies like fire, EMS, or public health do not want to participate in the fusion center process
- All the information that these non-law enforcement agencies could provide could be obtained in other ways even if it takes longer to obtain
- Non-law enforcement agency personnel do not have security clearances so they cannot be part of any analysis

- There is not enough work for these agencies to be involved
- Terrorism investigations are law enforcement-based operations that can be compromised by non-law enforcement agencies
- There is not enough space available to house other agencies in the fusion center
- The relationships with others are not established or valued
- Technology solutions are too expensive to initiate and maintain

In fact, many of these doubts relate to the lack of research in working through these issues. Conducting research and a thorough evaluation of the needs of information sharing is something that many law enforcement-based fusion centers have not done. This lack understanding of the needs of the information-sharing system usually stems from the administrators of the fusion centers. Fusion center administration usually comes from backgrounds that are law-enforcement centric. Because of this, many have failed to see the possibilities that expanded capabilities of information sharing can produce.

The sensitive nature of the information housed and processed in fusion centers is of great concern to all who collect, analyze, or use the information. All consumers and producers of information should protect the sensitivity of information while still making it available to those who need it in a timely manner. Many current fusion center configurations do not possess an information sharing system to get vital information to non-participating agencies in a timely fashion. The information sharing process is a critical part of a fusion center's operation if the fusion center is to be effective. Most of the information-sharing systems that are currently established in fusion centers were built to share information between law enforcement agencies only.

To promote information flow both between non-law enforcement agencies and fusion centers, current law-enforcement centric systems will need to be modified or new systems should be established. The goal of fusion centers should be to have input from a wide variety of information sources creating tips and leads that either support or start an investigation. This information can also provide the means to prevent deter or intervene into a criminal's intent. The ideas

and suggestions that are identified in this thesis outline the base upon which these new systems can be built. The traditional fusion center of the past is thought of as a law enforcement only facility, which focuses only on the terrorism aspect of a community or state. By utilizing new and innovative thinking, the fusion center of the future can become more robust information-sharing system and less of just a facility where people work. Most fusion centers do not encourage contributions from non-law enforcement agencies nor do they currently share information with many of these agencies. The need for change will increase as we are called upon to do more planning and preparing for responses between the different agencies. By sharing information between more agencies, the information-sharing system becomes more diverse through the inclusion of more partners and hazard identification. Through incorporation of the components listed in the thesis, a larger approach to fusion centers can be established.

One approach that can come from the inclusion of multi-discipline information- sharing systems is that of the All Hazards/All Crimes approach. Through the components of trust and technology, these non-law enforcement agencies can be connected through a virtual or technological connection to the systems within fusion centers. The administrators of current fusion centers must first build a trust of these new partners to establish a relationship, which will allow for information sharing occurring. The use of technology allows both security as well as access to these systems. Information technology administrators can track, limit, and approve all information sharing. This will serve as a positive to support the expansion of the number of agencies that can participate in the systems. This expansion will allow information sharing to develop additional roles for the fusion center such as supporting more natural and accidental event support for all agencies.

The advantage of an All Hazards/All Crimes would be that the access to information and the distribution of information would be greatly increased. Through secured portals, more agencies would be able to provide information

and thus would be able to receive information. The change in direction of the center must first start at the top of the law enforcement agencies involved in the fusion centers. This includes local, state, and federal agencies that will embrace the value of new partners, the assets, and information that they can bring to the information-sharing system. As new systems are developed to share information in a secured and enhanced fashion, fusion centers should look at who can provide new avenues of information. Through relationship building, the fusion center can work to include an information sharing system involving new work process such as virtual connections to the center, which will go beyond the traditional aspects of intelligence collection and analysis.

With the inclusion of the new agencies, the move to incorporate prevention and response activities into the daily operations of the fusion center will enhance the value of the investment by fusion center funding. DHS has been addressing the need for information sharing through both funding and technical assistance. The guidance from Congress has been that information sharing is an important part of the war on terrorism and should look for ways to increase its effectiveness.[47] The new role of fusion centers can provide a platform to reach well beyond the prevention phase of their traditional interests. The need to address the response phase of incidents will have an impact on fusion center development in the future. The inclusion of duties such as development and maintenance of Buffer Zone Protection Plans and critical infrastructure response plans can provide additional work and production for fusion centers. The importance of having information on threats and vulnerabilities should be coupled with the ability to translate that into a prevention and response model. The fusion center provides a platform for receiving information, processing the information and distribution of that information in a variety of means. If threats are identified the fusion center can also provide a central point for coordination of assets to protect and respond to these threats.

[47] Congressional Research Service, "A Summary of Fusion Centers: Core Issues and Options for Congress," September 19, 2007, 5.

The multi-discipline fusion center of the future can become the information and intelligence section for emergency operations centers through the incident command system. There will be a need for analysis of information during events that multi-discipline fusion centers can provide through their existing networks. The ability to push information out to units in the field from these centers can also provide an enhanced platform for an overall more effective system.

As fusion centers look to enhance their capabilities, the inclusion of non-law enforcement agencies in their information sharing systems will provide a greater capability for all types of events. Through a change in goals and understanding by all agencies that provide information, assets, and staff fusion centers can look at expanded roles and positions that make themselves a more valuable asset to communities and states. The key to the future success of fusion centers will rely on the implementation of the components of interoperability, governance, relationships, megacommunities, trust, standard operating procedures, technology, and leadership. While many current fusion centers have some of these components, the incorporation of the aspects of all those identified is needed to be successful.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

The interviews for the research on this thesis were conducted by telephone after the subjects were sent a copy of the questionnaire. For this research, the respondents nor their agencies are not identified in the thesis. This provided for a greater dialogue with the interviewees on some subjects that might have been sensitive in nature. There were ten agencies selected for the interviews. Only eight of the ten agencies responded positively to the request for an interview. One agency did not respond and another refused to participate after getting more information on the subject of the thesis. Of the eight agencies that did participate in the interviews each was contacted by phone prior to being sent a questionnaire. This allowed for a dialogue on the nature and scope of the interview. A time was then set up to conduct the phone interview and the informed consent form was faxed back. The information obtained in the interviews was very positive and provided excellent feedback to support further research. There were ten questions on the interview, which were designed to allow the interviewee to provide as much information as they wished. Questioned asked ranged from the agencies that the center was currently sharing information with to the types of technology that was being used. Throughout the interviews of the eight agencies the questions, we refined to focus the responses to the desired subjects.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

The survey that was conducted was based on the responses from the interviews. The interviews had been focused on the fusion centers who currently posses the information collection and dissemination processes. The intent of the survey was to seek responses from those outside of the fusion centers to gauge the effectiveness or perception of how well the fusion centers were sharing information. The survey was made accessible to the Urban Area Security Initiative list server for all state and local participants. There were no controls placed on who from this list could respond or direction to specific disciplines. One hundred forty seven responses were used in the data collection. The questions on the survey were developed around responses by the fusion center interviews. Information about the effectiveness of information sharing systems and participation by non-law enforcement agencies were the central focus. Responses supported the hypothesis that information sharing is not taking place as we would hope. While inside the fusion centers the perception is that they are getting information out, those on the outside do not feel they are getting enough information. The responses also indicate there is a gap in where non-law enforcement agencies can get information. In addition, there is a lack of the components identified in the recommendations of this thesis that are necessary for a successful information-sharing environment to exist. The survey indicates that there should be further research and evaluations of the current relationships between fusion centers and the non-law enforcement community.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

AT&L Knowledge Sharing System–Home. https://akss.dau.mil/askaprof-akss/qdetail2.aspx?cgiSubjectAreaID=15&cgiQuestionID=20023 (accessed November 28, 2008).

Carafano, James J. "Terrorist Intelligence Centers Need Reform Now." *The Heritage Foundation*, May 10, 2004, http://www.heritage.org/Research/HomelandDefense/em930.cfm/ (accessed January 5, 2008).

Clinton, William J. "Criminal Intelligence Systems Operating Policies." *Executive Order 12291*. 1998 Policy Clarification. 1993 Revision and Commentary.

Congressional Research Service. "A Summary of Fusion Centers: Core Issues and Options for Congress." September 19, 2007.

Covey, Stephen M. R. *The Speed of Trust. The One Thing That Changes Everything*. New York: Free Press, 2006.

Gerencser, Mark, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly. *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together*. New York, Palgrave Macmillan, March 2008.

Grance, Timothy, Marc Stevens, and Marissa Myers. *Guide to Selecting Information Technology Security Products: Recommendation of National Institute of Standards and Technology*. Special Publication 800-36. Maryland, National Institute of Standards and Technology, October 2003, http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf (accessed January 10, 2008).

Harman, Jane. Chairman of the House. *The Way Forward on Fusion Centers: Challenges and Strategies for Change*. Committee on Homeland Security Subcommittee on Intelligence, Information Sharing & Terrorism Risk Assessment. Thursday, September 27, 2007.

"The Homeland Security Information Network: An Update on DHS Information Sharing Efforts." Statement for the Record before the House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, September 13, 2006.

McDaniel, Michael C., Emad (Al) Shenouda, and M. John Bustria. “The Functional Desks as Collaborative Mechanisms in the Michigan Intelligence Operations Center.” *Homeland Security Affairs*, Supplement no. 2 (2008), http://www.hsaj.org/?article=supplement.2.4 (accessed January 5, 2009).

McKay, Jim. “The Security Shuffle.” *Government Technology*, November 4, 2005, http://www.govtech.net/magazine/channel_story.php/97157 (accessed January 5, 2008).

National Commission on Terrorist Attacks upon the United States. “Final Report on 9/11 Commission Recommendations.” Thomas H. Kean and Lee H. Hamilton. *The 911 Commission Report.* Washington, DC, 2004.

National Governors Association Center for Best Practices. “Establishing State Intelligence Fusion Centers.” July 12, 2005, http://www.nga.org/portal/site/nga/menuitem.9123e83a1f6786440ddcbeeb501010a0/?vgnextoid=560a6c6721115010VgnVCM1000001a01010aRCRD&vgnextchannel=4b18f074f0d9ff00VgnVCM1000001a01010aRCRD (accessed November 10, 2008).

National TEW Resource Center. *Resource Guide: Book One*: *TEW Concept and Overview*. Los Angeles, CA: National TEW Resource Center, January 2005, http://www.ojp.usdoj.gov/odp/docs/Resourcebook1_TEW.pdf (assessed October 22, 2008).

Neal, Judi. *Edgewalkers: People and Organizations that Take Risks, Build Bridges, and Break New Ground.* Annotated ed. Westport: Praeger Publishers; October 30, 2006.

Thomas, Dan. “Technology Strategy for Second Generation Fusion Centers.” *IPublic .org.* March 28, 2008, http://www.ipublic.org/wiki/index.php/Technology_strategy_for_second_generation_fusion_centers (accessed November 13, 2008).

United States Congress. Intelligence Reform and Terrorism Prevention Act of 2004. Public Law 108-458-December 17, 2004.

United States Department of Justice. “Baseline Capabilities for State and Major Urban Area Fusion Centers.” *Global Justice Information Sharing Initiative*, September 2008.

_____. “Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era.” *Global Justice Information Sharing Initiative*, April 2006.

United States Department of Homeland Security. *National Infrastructure Protection Plan.* Washington, DC: Government Printing Office, 2006.

_____. *National Infrastructure Protection Plan. Constellation/Automated Critical Asset Management System.* http://www.dhs.gov/xinfoshare/programs/gc_1190729724456.shtm, (accessed March 5, 2009).

_____. *National Infrastructure Protection Plan. Protected Critical Infrastructure Information Program.* http://www.dhs.gov/xinfoshare/programs/gc_1193089801658.shtm (accessed March 6, 2009).

United States, President George W. Bush. *National Strategy for Information Sharing*. The Whitehouse, October 2007.

Wikipedia. http://en.wikipedia.org/wiki/Interoperability (accessed November 27, 2008).

_____. http://en.wikipedia.org/wiki/Standard (accessed December 5, 2008).

WiMAX. http://www.wimax.com/education (accessed March 7, 2009).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Richard Bergin
   Naval Postgraduate School
   Monterey, California

4. Robert Josefek
   Naval Postgraduate School
   Monterey, California

5. Jon Hannan
   Charlotte Fire Department
   Charlotte, North Carolina